Steuerung von Wissensrisiken

Dissertation

zur Erlangung des Grades
Doktor der Wirtschaftswissenschaften (Dr. rer. pol.)

der Juristischen und Wirtschaftswissenschaftlichen Fakultät
der Martin-Luther Universität Halle-Wittenberg

vorgelegt von

Dipl. Kfm. Florian Bayer

Gutachter: Prof. Dr. Ronald Maier, Prof. Dr. Gerhard Kraft

Tag der Verteidigung: 5. Februar 2009

Vorwort

Bedingt durch den immer evidenteren Wandel zur Wissensgesellschaft und die zunehmende Regulierung hinsichtlich Risiken wurden in den vergangenen Jahren zunehmend Initiativen zu Wissensmanagement- und Risikomanagement in Unternehmen eingeführt, wobei deren Zielstellungen zum Teil konträr sind und die Integration dieser Initiativen in der Regel nicht gegeben ist. So nehmen die Ansätze zum Wissensmanagement nahezu eine durchgängig positive Grundhaltung zu einer umfassenden Erhöhung der Transparenz, Verfügbarmachung und Verteilung von Wissen ein, ohne dabei entsprechende "Risiken und Nebenwirkungen" zu betrachten, während die Ansätze im Kontext des Risikomanagements, Risiken, die Wissen als Ressource betreffen, außen vor lassen.

Dieses Spannungsfeld hat mich in den letzten vier Jahren am Lehrstuhl für Wirtschaftsinformatik an der Martin-Luther Universität, an der diese Arbeit entstanden ist, beschäftigt. Für Wissensmanagement selbst habe ich mich schon während meines Studiums an der Universität Regensburg begeistert und aus diesem Grund auch meine Diplomarbeit in diesem Themenkomplex geschrieben. Die Relevanz des Themengebiets wurde mir insbesondere im Rahmen eines Forschungsprojektes deutlich, in dem der Wissenstransfer zwischen Unternehmen, die sich in einem kooperativen Wettbewerb (Coopetition) befinden, deutlich, da dort zentrale Fragestellungen im Hinblick auf die Grenzen und potentielle Risiken der interorganisationalen Zusammenarbeit aufkamen.

Die vorliegende Arbeit wäre ohne die Unterstützung einer Reihe an Personen, denen ich nachfolgend danken möchte, nicht möglich gewesen.

Ganz besonders möchte ich meinem Doktorvater Herrn Prof. Dr. Ronald Maier danken, der ein hervorragendes Forschungsumfeld sicherstellte, in zahlreichen Diskussionen seine Kompetenzen und Ideen einbrachte und vor allem auch durch seine Fähigkeit, Menschen zu motivieren, das Thema voranbrachte. Weiterhin möchte ich Herrn Prof. Dr. Gerhard Kraft für die Übernahme des Koreferats und seine wertvollen Anregungen danken. Weiterhin durfte ich in einem Team arbeiten, in dem nicht nur die eigenen Arbeiten, sondern auch die Arbeiten der Kollegen jederzeit präsent waren, vielfach diskutiert und gemeinsam weiterentwickelt wurden. Aus diesem Grund gilt mein Dank meinen ehemaligen Kollegen Thomas Hädrich, René Peinl, Stefan Thalmann und Mathias Trögl.

Weiterhin danke ich der Deutschen Forschungsgemeinschaft für die Förderung der empirischen Studie kNOwRISK. Hinsichtlich dieser Studie gilt mein besonderer Dank auch den beiden studentischen Hilskräften Nadine Amende und Marcus Behrendt für ihren Einsatz und ihr Durchhaltevermögen bei der Telefonakquise von Unternehmen, gerade in einer Zeit, in der empirische Erhebungen bedingt durch die Informationsflut immer schwieriger werden. In diesem Zusammenhang möchte ich auch Herrn Markus Bachmeyer von der Creditreform Halle für die Bereitstellung der Unternehmensadres-

sen und die Unterstützung bei deren Ziehung bedanken. Im Hinblick auf die statistische Auswertung möchte ich weiterhin Frau Prof. Dr. Claudia Becker von der Universität Halle sowie Henry Dannenberg und Olaf Neubert vom Institut für Wirtschaftsforschung Halle für ihre wertvollen Hinweise danken.

Mein größter Dank gilt meinen Eltern, Ingeborg und Erhard Bayer, die meine akademische Ausbildung erst ermöglicht haben und mir jederzeit den Rücken stärkten sowie meiner Freundin Ivonne Hubmacher für ihr großes Verständnis und ihr wundervolles Einfühlungsvermögen.

Florian Bayer

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
AG	Aktiengesellschaft
AktG	Aktiengesetz
BBA	British Bankers' Association
BetrVG	Betriebsverfassungsgesetz.
BGH	Bundesgerichtshof
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
CC	Common Criteria
CobiT	Control Objectives for Information and related Technology
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAC	Discretionary Access Control
DIN	Deutsche Institut für Normung
DRS	Deutsche Rechnungslegungs Standards
DRSC	Deutsche Rechnungslegungs Standards Committee
EBIT	earnings before interest and taxes
et al.	und andere
etc.	et cetera
EU	Europäische Union
EVA	Economic Value Added
f	folgende
FASB	Financial Accounting Standards Boards
ff	fortfolgende
FTP	File Transfer Protocol
GARP	Global Association of Risk Professionals
GebrMG	Gebrauchsmustergesetz
GenG	Genossenschaftsgesetz
GeschmMG	Geschmacksmustergesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GuV	Gewinn- und Verlustrechnung
HalblSchG	Halbleiterschutzgesetz
HCROI	ROI of Human Capital
HFLI	High Frequency Low Impact
HGB	Handelsgesetzbuches
HTTP	Hypertext Transfer Protocol
i.d.R.	in der Regel
IAS	International Accounting Standard
IASB	International Accounting Standards Board
IASC	International Accounting Standards Committee
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IDW PS	IDW Prüfstandard
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standards

IP	Intellectual Property
ISMS	Informationssicherheits-Managementsystems
ISO	International Organization for Standardization
IT	Informationstechnologie
ITSEC	Information Technology Security Evaluation Criteria
KG	Kommanditgesellschaft
KGaA	Kommanditgesellschaft auf Aktien,
KonTraG	Gesetz zur Transparenz und Kontrolle im Unternehmensbereich
KRI	Key Risk Indicator
LFHI	Low Frequency High Impact
MAC	Mandatory Access Control
MarkenG	Markengesetz
NIST	Institute of Standards and Technology
ODRL	Open Digital Rights Language
PatG	Patentgesetz
POP	Post Office Protocol
RBAC	Role Based Access Control
RM	Risikomanagement
ROA	Return on Assets
ROI	Return on Investment
ROSI	Return on Security Investments
SolvV	Solvabilitätsverordnung
SOMAP	Security Officers Management and Analysis Project
SoSchG	Sortenschutzgesetz
SOX	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
Tab.	Tabelle
TCSEC	Trusted Computer System Evaluation Criteria
TRIPS	Trade Related Aspects of Intellectual Property Rights
Tz.	Textziffer
UrhG	Urhebergesetz
URL	Unified Resource Locator
USB	Universal Serial Bus
US-GAAP	U.S.Generally Accepted Accounting Principles
usw.	und so weiter
UWG	Gesetz gegen unlauteren Wettbewerb
VoIP	Voice over Internet Protocol
WM	Wissensmanagement
XML	Extensible Markup Language
XrML	eXtensible rights Markup Language
z.B.	zum Beispiel

1 Einleitung

1.1 Problemstellung

Der von Peter Drucker (1992, 95) prognostizierte Wandel hin zur Wissensgesellschaft zeigt sich immer deutlicher darin, dass Aktivitäten, Produkte und Dienstleistungen in Unternehmen zunehmend wissensintensiver geworden sind und der Anteil an wissensintensiver Arbeit steigt (Wolff 2005, 38). Wissensbezogene Ressourcen als Teil organisatorischer Ressourcen können einen entscheidenden Einfluss auf die Wettbewerbsposition von Unternehmen haben (Mentzas et al. 2003, 1). Mit der gestiegenen Wissensintensität und dem erhöhten Bewusstsein für Wissen als Ressource sind seit der Entwicklung von ersten Ansätzen zum Wissensmanagement (WM) durch Sveiby und Lloyd (1987) und Wiig (1988) und ihrer Verbreitung z.B. durch Nonaka (1991), Blackler (1995), Davenport und Prusak (1998), Probst et al. (1998) und Willke (1998) in vielen Unternehmen und Organisationen WM-Initiativen und WM-Systeme eingeführt worden, über die im Rahmen von Fallstudien und breit angelegten Erhebungen berichtet wurde[1]. Diese haben beispielsweise zum Ziel, Wissen transparent zu machen, zu explizieren, zu kodifizieren und auch im Unternehmen oder über die Unternehmensgrenzen hinaus zu verteilen.

Neben der gestiegenen Wissensintensität ist auch eine verstärkte Risikoorientierung der Unternehmen zu beobachten, wobei der Umgang mit Risiken seit langem als integraler Bestandteil der Unternehmensführung angesehen wird, da unternehmerische Handlungen generell risikobehaftet sind (Wall 2001, 207). Dabei haben in der Vergangenheit die gestiegene Dynamik des Unternehmensumfeldes, die Globalisierung des Wettbewerbs, die zunehmende Vernetzung von Informations- und Kommunikationstechnologien (Zech 2002, 35) sowie nicht zuletzt zahlreiche Unternehmenskrisen (von Hohnhorst 2002, 93; Kern 2003, 35) die Zunahme des Bewusstseins für Risiken zur Folge und dazu geführt, dass neben zahlreichen anderen, teils branchenspezifischen Initiativen[2] 1998 das Gesetz zur Transparenz und Kontrolle im Unternehmensbereich (KonTraG) verabschiedet wurde. Durch dieses Gesetz werden Kapitalgesellschaften dazu verpflichtet, in Bezug auf die Risikofrüherkennung Maßnahmen zu ergreifen und ein Überwachungssystem einzurichten (Picot 2001, 5ff; Kern 2003, 38ff). Daher haben sich in den vergangenen Jahren viele Unternehmen mit Risikomanagement (RM) auseinandergesetzt und entsprechende Initiativen eingeführt. Jedoch erfolgt in den verschiedenen RM-Ansätzen trotz der hohen Bedeutung der Ressource Wissen für die Begründung der Wettbewerbsposition bisweilen keine explizite und systematische Auseinandersetzung mit Risiken, die die Ressource

[1] vgl. z.B. (APQC 1996; Bullinger et al. 1997; Chase 1997; Delphi 1997; Davenport, Prusak 1998; Heisig, Vorbeck 1998; Ruggles 1998; Bach et al. 1999; Döring-Katerkamp, Trojan 2000; Antoni, Sommerlatte 2001; Döring-Katerkamp, Trojan 2001; Mertins et al. 2001; Maier 2004)

[2] Beispiele sind: Basel II für die Bankwirtschaft; Solvency II für die Versicherungswirtschaft oder der Sarbanes-Oxley Act.

Wissen betreffen, sondern eine primäre Betrachtung von Markt- und Kreditrisiken. Ebenso wird in den Ansätzen des WM nur selten thematisiert, wie Wissen gesichert werden kann, um somit auch wissensbasierte Wettbewerbsvorteile zu sichern (Coleman, Casselman 2004, 2; Desouza, Vanapalli 2005, 76).

Auch Unternehmen, die WM-Initiativen oder WM-Systeme eingeführt haben, sind von Wissensrisiken betroffen. Die Initiativen und Systemeinführungen betonen die Vorteile der besseren Zugänglichkeit von Wissen. Jedoch sind mit der Erhöhung der Transparenz und Verteilung von Wissen auch Risiken verbunden, denen nicht systematisch Beachtung geschenkt wird. Es ist zu vermuten, dass bedingt durch das fehlende Management dieser Risiken Potentiale im Einsatz von WM-Instrumenten und -Systemen derzeit nicht ausgeschöpft werden. Ein systematisches RM kann sowohl einen restriktiveren Umgang mit Wissen nahe legen, falls die Risiken unterschätzt werden, als auch einen offeneren Umgang, falls diese zu hoch eingeschätzt werden. Somit bestehen in Bezug auf Risiken, die die Ressource Wissen betreffen, sowohl aus der Perspektive des WM als auch aus der Perspektive des RM Forschungslücken, die den thematischen Rahmen der Arbeit bilden.

1.2 Zielsetzung und Forschungsfragen

Im Rahmen dieser Arbeit werden die Wirtschaftswissenschaften als angewandte Wissenschaft verstanden, deren primäres Erkenntnisziel darin besteht, ein wissenschaftlich fundiertes Handeln in der Praxis zu ermöglichen, indem Methoden, Modelle und Handlungsempfehlungen zur Lösung unternehmerischer Problemstellungen bereitgestellt werden (Ulrich 1984, 178ff). Im Hinblick auf die Ziele der Wissenschaft unterscheidet Schanz allgemein zwischen einem theoretischen Wissenschaftsziel, das sich aus dem Erkenntnisinteresse ableitet, und einem praktischen Wissenschaftsziel, das aus dem Gestaltungsinteresse resultiert (Schanz 1988, 6). Legt man eine feinere Unterteilung zugrunde (siehe Abb. 1), so kann zwischen einem essentialistischen, theoretischen, pragmatischen und normativen Wissenschaftsziel unterschieden werden (Chmielewicz 1979, 17ff). Dabei soll durch das erstgenannte Ziel mittels Begriffslehre die Essenz der Dinge möglichst exakt in Begriffe und Definitionen gefasst werden. Im Rahmen der Wirtschaftstheorie, die mit dem theoretischen Wissenschaftsziel korrespondiert, sollen Ursache- und Wirkungszusammenhänge erklärt werden und aus den Begriffen Aussagen und Theorien gebildet werden. Das pragmatische Wissenschaftsziel korrespondiert mit dem Gestaltungsinteresse und wird dadurch erreicht, dass aus den Ursache- und Wirkungszusammenhängen Ziel-Mittel Relationen abgeleitet werden, auf deren Basis Handlungsempfehlungen entwickelt

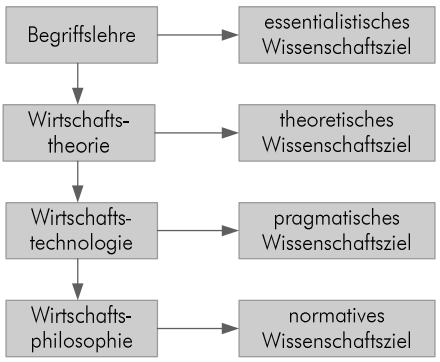


Abb. 1 Wissenschaftsziele

werden können. Normative Wissenschaftsziele, die eine philosophische Ausrichtung aufweisen, haben die Abgabe und Begründung von Werturteilen zum Gegenstand (Chmielewicz 1979, 17ff).

Bezogen auf die zuvor dargestellte Problemstellung besteht die allgemeine Zielsetzung dieser Arbeit darin, die zum aktuellen Stand der Forschung nur gering und nicht systematisch betrachteten Wissensrisiken auf der Ebene der operativen Geschäftsprozesse zu analysieren und Erkenntnisse zu Maßnahmen bzgl. der Risikosteuerung zu gewinnen. Durch die gewonnenen Erkenntnisse soll das Handlungsrepertoire von Unternehmen in Bezug auf den Umgang mit Wissensrisiken erweitert werden und so zu einer Verbesserung der Produktivität von wissensintensiven Aktivitäten und Prozessen beigetragen werden. Die in Abb. 1 dargestellten Wissenschaftsziele lassen sich auf folgende allgemeine Zielstellungen und entsprechende Forschungsfragen übertragen.

(I) Systematisierung des Konzeptes Wissensrisiko (essentialistisches Wissenschaftsziel): Das essentialistische Ziel dieser Arbeit besteht demnach darin, das Konzept Wissensrisiko zu definieren und auf Basis der Literatur Wissensrisiken und entsprechende Gegenmaßnahmen zu identifizieren. Darüber hinaus sollen die Zusammenhänge analysiert und systematisiert werden.

(Ia) *Welche wissensbezogenen Ressourcen bestehen und wie kann ihr Wert ermittelt werden?*
Ausgehend von der These, dass sich Wissensrisiken auf Ressourcen, die auf Wissen basieren, auswirken, soll durch die Beantwortung dieser Forschungsfrage aufgezeigt werden, welche Arten wissensbezogener Ressourcen in Unternehmen bestehen und wie eine Wertbeimessung erfolgen kann. Eine Wertbeimessung ist insbesondere dann bedeutend, wenn Steuerungsmaßnahmen effizient allokiert werden sollen.

(Ib) *Welche Wissensrisiken bestehen und wie können sie systematisiert werden?*
In der bisherigen Forschung zu Wissensrisiken wurde noch keine umfassende Untersuchung vorgenommen, sondern vielmehr auf spezifische Teilaspekte, wie z.B. Risiken aus Fluktuation, fokussiert. Im Rahmen dieser Arbeit soll daher aufgezeigt werden, welche Risiken in Bezug auf Personen, Prozesse, IT-Systeme und externe Faktoren bestehen.

(Ic) *Welche Maßnahmen zur Steuerung von Wissensrisiken bestehen und wie können sie systematisiert werden?*
Ebenso wie die Forschung zu Wissensrisiken steht auch die Forschung zu Steuerungsmaßnahmen an den Anfängen und stellt auf spezifische Teilaspekte ab. Im Rahmen dieser Arbeit sollen daher Steuerungsmaßnahmen aus verschiedenen Forschungsströmungen analysiert und adaptiert werden, um so zu einer Erweiterung des Handlungsrepertoires für Unternehmen beizutragen.

(II) Erklärung der Zusammenhänge (theoretisches Wissenschaftsziel): Im Rahmen einer empirischen Studie sollen die aus der Theorie gewonnenen Erkenntnisse erklärt werden, indem die Re-

levanz von Wissensrisiken und die Wirkung der Steuerungsmaßnahmen überprüft werden. Diese Ursache- und Wirkungszusammenhänge sollen weiterhin durch die Identifikation unternehmensinterner und -externer Einflussfaktoren erklärt werden. Im Einzelnen sind folgende Forschungsfragen diesem Wissenschaftsziel zuzuordnen.

(IIa) *Welche Wissensrisiken sind für Unternehmen relevant und wie gut lassen sie sich steuern?*

Auf Basis der empirischen Studie soll analysiert werden, welche Wissensrisiken für Unternehmen von Relevanz sind und wie gut die in der Studie eingeschlossenen Maßnahmen in Unternehmen gesteuert werden können. Durch die Beantwortung dieser Forschungsfrage sollen potentielle Handlungsbedarfe identifiziert werden.

(IIb) *Welche Austauschbeziehungen bzw. negativen Effekte gehen mit dem Ergreifen von Steuerungsmaßnahmen einher?*

Ausgehend davon, dass sich Risiken auch aus einer potentiellen Übersteuerung ergeben können soll durch die Beantwortung dieser Forschungsfrage aufgezeigt werden, welche potentiellen negativen Effekte das Ergreifen von Steuerungsmaßnahmen auf erwünschte Prozesse haben kann bzw. welche weiteren Wissensrisiken potentiell hervorgerufen werden können. Durch diese Analyse soll eine effiziente Steuerung dieser Risiken ermöglicht werden.

(IIc) *Welche Faktoren beeinflussen den Erwartungswert von Wissensrisiken bzw. die Notwendigkeit von Steuerungsmaßnahmen?*

Bedingt durch Größen- und Branchenunterschiede stellen Unternehmen einen sehr heterogenen Untersuchungsgegenstand dar, weshalb Zusammenhänge vielfach nicht verallgemeinerbar sind. Aus diesem Grund sollen im Rahmen dieser Arbeit unternehmensexterne und -interne Faktoren ermittelt werden, die auf die Eintrittswahrscheinlichkeit und das Schadensausmaß von Wissensrisiken einerseits und den Bedarf der Steuerung andererseits Einfluss nehmen.

(III) Erarbeitung von Handlungsempfehlungen (pragmatisches /normatives Wissenschaftsziel):

Unter Integration der essentialistisch und theoretisch gewonnenen Erkenntnisse sollen Empfehlungen erarbeitet werden, wie der Prozess des Wissensrisikomanagements unterstützt werden kann. Dies betrifft im Einzelnen die Methoden zur Identifikation und Bewertung von Wissensrisiken, Aussagen zur Eignung oder zu potentiellen Austauschbeziehungen bzw. negativen Effekten der Steuerungsmaßnahmen sowie Möglichkeiten der Implementierung in der Aufbau- bzw. Ablauforganisation von Unternehmen. Die Handlungsempfehlungen korrespondieren primär mit dem Gestaltungsinteresse und somit mit dem pragmatischen Wissenschaftsziel. Da auch Werturteile Gegenstand der Arbeit sind, wird sekundär auch das normative Wissenschaftsziel verfolgt.

(IIIa) *Wie kann das Management von Wissensrisiken in Unternehmen unterstützt werden?* Ausgehend vom Prozess des Wissensrisikomanagements soll durch die Beantwortung dieser Forschungsfrage aufgezeigt werden, durch welche Methoden und Instrumente die verschiedenen Aufgaben des Wissensrisikomanagementprozesses, die von der Identifikation über die Bewertung, Steuerung und Überwachung von Wissensrisiken reichen, unterstützt werden können.

(IIIb) *Wie kann das Management von Wissensrisiken in Unternehmen implementiert werden?* Ein effizientes Management von Wissensrisiken bedarf einer entsprechenden Implementierung in Unternehmen. Durch die Beantwortung dieser Forschungsfrage soll aufgezeigt werden, wie eine Einbettung in die Aufbau- und Ablauforganisation von Unternehmen erfolgen kann.

Nachdem die Wissenschaftsziele und korrespondierenden Forschungsfragen erörtert wurden, werden im folgenden Abschnitt der Aufbau der Arbeit und die jeweils zugrunde liegende Methodik erörtert.

1.3 Methodisches Vorgehen und Aufbau der Arbeit

Die in Abschnitt 1.2 erörterten Ziele spiegeln sich wie in Abb. 2 dargestellt auch im Aufbau der Arbeit wider. So werden im Anschluss an die Einleitung die theoretischen Grundlagen der Arbeit, die für das Konzept Wissensrisiko von Relevanz sind, analysiert. Als Methodik liegt diesem Teil der Arbeit eine Literaturanalyse zugrunde. Im Einzelnen werden in Kapitel 2 ausgehend vom ressourcenbasierten Ansatz wissensbezogene Ressourcen und deren Wert für Unternehmen erörtert. Diese Ressourcen bilden den zentralen Gegenstand, auf den sich Wissensrisiken nach dem dieser Arbeit zugrunde liegenden Verständnis auswirken. In Kapitel 3 werden unterschiedliche Perspektiven auf Risiko und die Kernaufgaben des RM erörtert, während in Kapitel 4 als spezielle Teildisziplin des RM IT-Risiken und die entsprechenden Maßnahmen sowie eine Auswahl an Standards betrachtet werden. In Kapitel 5 wird auf Basis der Kapitel 2 bis 4 das Konzept Wissensrisiko, das aus den Teilkonzepten Wissensverlust, -diffusion, -transfer und -qualität besteht, erarbeit. Im Ergebnis soll dieser Teil der Arbeit der Erreichung des essentialistischen Ziels dienen und eine Systematisierung der Wissensrisiken und Steuerungsmaßnahmen in entsprechende Kataloge zum Ergebnis haben.

Die Kapitel 6 und 7 dienen primär zur Erklärung der Zusammenhänge zwischen Wissensrisiken und Steuerungsmaßnahmen und folgen dem theoretischen Wissenschaftsziel. Als Methodik wird eine mehrstufige empirische Untersuchung durchgeführt, die einem explorativen Ansatz folgt[3]. Das entsprechende Design der Studie, das u.a. die Ziehung der Stichprobe, Pretests und die Erstellung des Interviewleitfadens umfasst, ist Gegenstand von Kapitel 6, während die Auswertung auf Basis de-

[3] Die Durchführung der empirischen Studie wurde durch die Deutsche Forschungsgemeinschaft unter dem Kennzeichen MA3895/1-1 gefördert.

skriptiver, induktiver und multivariater statistischer Verfahren den Gegenstand von Kapitel 7 bildet. Dabei sollen im Ergebnis in einer breiten empirischen Studie (n=129) auf der Basis von Telefoninterviews und strukturierten Interviewleitfäden quantitative und qualitative Erkenntnisse zur Relevanz von Wissensrisiken und deren Steuerung in der Praxis gewonnen werden. Unter Zugrundelegung der aus dieser Studie gewonnenen Erkenntnisse werden in einer unternehmensübergreifenden (n=12) und einer unternehmensinternen vertiefenden Studie (n=66) spezifische Sachverhalte erörtert. Im Rahmen der Auswertung sollen auch erste Erkenntnisse gewonnen werden, die mit dem Gestaltungsinteresse einhergehen und somit mit dem pragmatischen Wissenschaftsziel korrespondieren.

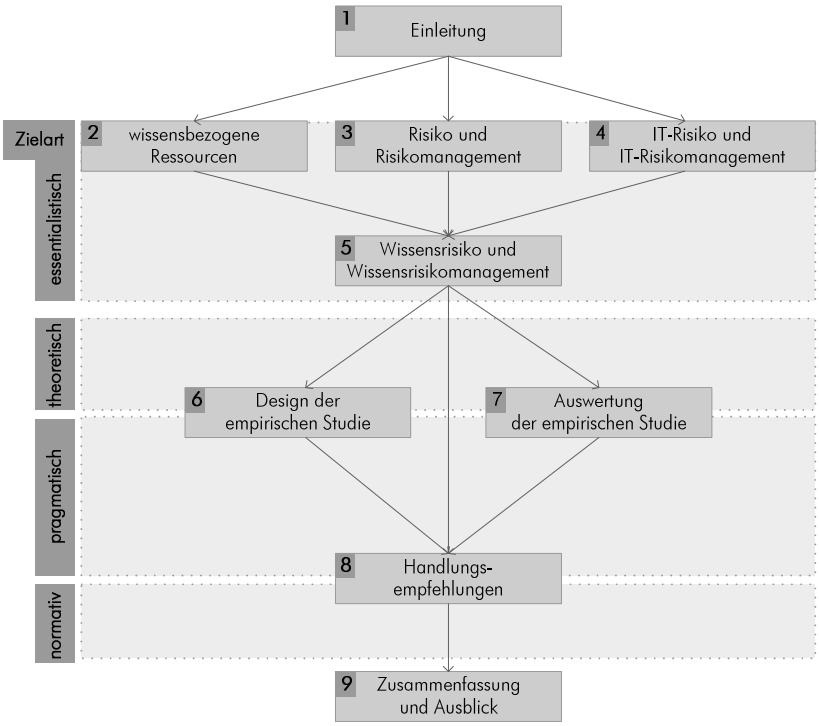


Abb. 2 Aufbau der Arbeit

In Kapitel 8 der Arbeit werden die aus der Literaturanalyse und der mehrstufigen empirischen Studie gewonnenen Erkenntnisse integriert betrachtet und in Handlungsempfehlungen überführt, die u.a. den Einsatz von Steuerungsmaßnahmen oder die Implementierung des Managements von Wissensrisiken in der Aufbau- und Ablauforganisation von Unternehmen betreffen. Dabei dient dieses Kapitel sowohl zur Erreichung des pragmatischen Wissenschaftsziel als auch zur Realisierung des normativen Wissenschaftsziels, indem Werturteile integriert werden. Insgesamt liegt der Arbeit als Methodik zum einen eine Literaturanalyse zugrunde, die zur theoretischen Fundierung der Kapitel 2 bis 4 und zur Erarbeitung des Konzeptes Wissensrisiko dient. Zum anderen werden die aus der Literatur gewonnenen Erkenntnisse im Rahmen einer empirischen Studie in der Praxis reflektiert. Sowohl die Erkenntnisse der Literaturanalyse als auch die aus der empirischen Studie fließen in Handlungsempfehlungen ein. Nachdem der Aufbau der Arbeit erläutert wurde, werden in nachfolgendem Abschnitt ausgehend von der ressourcenbasierten Sichtweise auf Unternehmen wissensbezogene Ressourcen analysiert.

2 wissensbezogene Ressourcen und deren Bewertung

Der ansteigenden Bedeutung von Wissen für die Wertschöpfung sowie für die Generierung bzw. Erhaltung von Wettbewerbsvorteilen wird zunehmend auch im strategischen Management durch die Entwicklung des wissensbasierten Ansatzes zur Unternehmensführung Rechnung getragen. Ausgehend von der Markt- und Ressourcenorientierung als grundlegende strategische Ausrichtungen ist der wissensbasierte Ansatz der ressourcenorientierten Perspektive auf Unternehmen zuzuordnen und hat sich aus dieser entwickelt. Der wissensbasierte Ansatz stellt die Verortung des Managements von Wissensrisiken in der strategischen Unternehmensführung dar und ist daher der Hauptgegenstand dieses Kapitels. In Abschnitt 2.1 wird demzufolge zunächst ausgehend von der Ressourcenorientierung eine allgemeine Betrachtung von Ressourcen vorgenommen. Im Anschluss daran wird speziell auf die Besonderheiten der Ressource Wissen eingegangen (siehe 2.2). Da ein gezielter Umgang mit Risiken einer Wertbeimessung der betroffenen Ressourcen bedarf, werden in Abschnitt 2.3 Ansätze zur Bewertung immaterieller und wissensbezogener Ressourcen betrachtet. Das Kapitel schließt mit einer Zusammenfassung und Diskussion (siehe 2.4).

2.1 Ressourcen als Werttreiber

Gegenstand des nachfolgenden Abschnitts stellt die Betrachtung von Ressourcen dar. Dazu werden zunächst Entwicklungen des strategischen Managements (siehe 2.1.1) dargestellt und in diesem Zusammenhang insbesondere auf die spezifischen Grundzüge des ressourcenbasierten Ansatzes eingegangen. Um die Begriffsvielfalt zwischen Ressourcen, Vermögenswerten und intellektuellem Kapital, die durch die verschiedenen involvierten Forschungsströmungen zustande kommt, zu reduzieren, erfolgt im Anschluss eine Abgrenzung dieser Begriffe (siehe 2.1.2). Abschließend wird eine Kategorisierung von Ressourcen vorgenommen (siehe 2.1.3).

2.1.1 Entwicklung des ressourcenbasierten Ansatzes

Das strategische Management bildete sich vor ca. 30-40 Jahren als eine eigene wissenschaftliche Disziplin heraus und hat seine Ursprünge in den amerikanischen Business Schools (z.B. Harvard), in denen es als Lehrfach eine integrative Klammer um die betriebswirtschaftlichen Fächer (z.B. Marketing, Finanzierung) bildete (Müller-Stewens, Lechner 2005, 8f). Gründe für ihre Entwicklung sind beispielsweise eine zunehmende Komplexität von Unternehmen, die auf das Aufkommen von Mehrproduktunternehmen zurückzuführen ist, veränderte Kostenstrukturen mit zunehmend fixen Kosten, die in der Forderung nach einer langfristigen Absatzsicherung resultierten oder die Zunahme der Umweltdynamik, die den Einsatz konventioneller Planungstechniken erschwerte und eine stärkere Außenorientierung erforderte (Hümmer 2001, 19ff; Bea, Haas 2005, 7ff). Zentrale Ursprungswerke die-

ser Disziplin sind die „Theory of Growth“ von Edith Penrose (1959), „Structure and Strategy“ von Alfred Chandler (1962), „Corporate Strategy“ von Igor Ansoff (1965) oder „The Concept of Corporate Strategy“ von Kenneth Andrews (1971). Ein erstes Konzept des strategischen Managements stellt das LCAG Framework dar, das später auch unter dem Namen SWOT-Analyse[4] bekannt wurde und Verbreitung fand (Learned et al. 1965, 170ff). Durch die SWOT-Analyse soll ein Ausgleich zwischen unternehmensinternen Stärken und Schwächen einerseits und unternehmensexternen Chancen und Bedrohungen erzielt werden. Trotz einer heterogenen Begriffsauffassung lässt sich ein Grundverständnis ableiten. Demnach zielt das strategische Management auf die Schaffung von Handlungsmöglichkeiten um den zukünftigen Erfolg der Unternehmung sicherzustellen und fokussiert dabei die Planung des Entwicklungspfades, der bei Veränderungen der Umwelt flexibel angepasst werden kann (Al-Laham 2003, 15). Das Ziel besteht darin, in einem dynamischen Umfeld die Überlebensfähigkeit von Unternehmen durch Anpassung zu sichern (zu Kryphausen-Aufseß 2004, 1383).

Dabei stellen die Markt- und Ressourcenorientierung die klassische Paradigmen des strategischen Managements dar, wobei für erstere das Structure-Conduct-Performance-Paradigma, das Wettbewerbsvorteile (performance) durch die Branchenstruktur (structure) und das strategische Verhalten des Unternehmens (conduct) erklärt, die Grundlage bietet (Bain 1968). Diese rigide Sichtweise der traditionellen Industrieökonomik wurde vorwiegend durch die Arbeiten von Porter[5] kritisiert und dahingehend erweitert, dass auch das Verhalten der Unternehmen am Markt die Branchenstruktur beeinflussen kann (Porter 1981, 611). Nach dieser auch als neue Industrieökonomik bezeichneten Sichtweise wird die Branchenstruktur nicht mehr als exogene Variable gesehen, sondern kann zur Erlangung einer überlegenen Wettbewerbsposition gezielt beeinflusst werden. Das von Porter entwickelte Fünfkräftemodell basiert auf dieser Annahmen und dient als Bezugsrahmen zur Analyse der Branchenattraktivität unter Beachtung der fünf Wettbewerbskräfte Verhandlungsmacht der Kunden, Verhandlungsmacht der Lieferanten, Einfluss von Substitutionsprodukten, Ausprägung von Eintrittsbarrieren und Wettbewerbsintensität (Porter 1980, 4). Auf der Grundlage der Analyse der Branchenstruktur können Unternehmen die generischen Strategien Kostenführerschaft, Differenzierung und Konzentration auf Schwerpunkte zur Sicherung ihrer Wettbewerbsposition einsetzen.

Aus der Kritik einer zu starken externen Fokussierung und zu geringen Beachtung unternehmensinterner Ressourcen, hat sich der ressourcenbasierte Ansatz entwickelt. Anders als der marktbasierte Ansatz gründet sich diese Sichtweise auf eine Vielzahl an Veröffentlichungen unterschiedlicher Vertreter. Als Begründer dieser Sichtweise[6] gilt Wernerfelt (1984), der auf den Arbeiten von Penrose

[4] LCAG steht für die Nachnamen der Entwickler des Instrumentes Learned, Christensen, Andrews und Guth, während die Abkürzung SWOT Strength, Weakness, Opportunity und Threat bedeutet.

[5] Zu den wesentlichen Modellen der marktorientierten Sichtweise zählen das Fünfkräftemodell (Porter 1980, 4), die Wertkette (Porter 1985, 36ff) und der Diamant (Porter 1990, 71f).

[6] Die Wurzeln reichen zurück bis Selznick (1957) und Penrose (1959). Selznick prägte in diesem Zusammenhang den Begriff „distinctive competencies“, der unternehmensspezifische Besonderheiten bezeichnet. Penrose propagierte die

(1959) und Andrews (1971) aufbaut und die Bedeutung von Ressourcen für den Unternehmenserfolg betont, jedoch keine Gestaltungsempfehlungen zum Umgang mit diesen Ressourcen gibt. Das Konzept wurde maßgeblich von Wernerfelt (1989) selbst, Barney (1991), Grant (1991) und Peteraf (1993) weiterentwickelt. Der Ressourcenbegriff ist in diesem Ansatz enger gefasst als das volkswirtschaftliche Begriffsverständnis der Theorie der Ökonomie, das die Produktionsfaktoren Arbeit, Kapital und Boden umfasst (Al-Laham 2003, 113). Demnach werden alle unternehmensspezifischen materiellen und immateriellen Güter, Systeme und Prozesse als Ressourcen angesehen. Als grobe Klassifizierung können materielle (z.B. Produktionsanlagen, Maschinen), immaterielle (z.B. Patente, Copyrights, Fähigkeiten) und finanzielle Ressourcen unterschieden werden (Barney 1991, 110f; Grant 2001, 111ff; Lev 2005, 300)[7]. Die zentrale These der ressourcenbasierten Sichtweise, nach der Unternehmen als Bündel von Ressourcen verstanden werden, besteht darin, dass die Einzigartigkeit, Wettbewerbsvorteile und Performanceunterschiede von Unternehmen durch eine unterschiedliche Ressourcenausstattung sowie Unterschiede bezüglich deren Qualität und Effizienz zu erklären sind (Hümmer 2001, 49; Müller-Stewens, Lechner 2005, 357). Als Prämissen liegen dieser These die Ressourcenheterogenität und -immobilität zugrunde, die sich auf historische Entwicklungen oder die Unvollkommenheit bzw. die Nichtexistenz von Faktormärkten zurückführen lassen, wobei nachhaltige Wettbewerbsvorteile eines Unternehmens aus dem Einsatz bzw. der Kombination einzigartiger unternehmensspezifischer Ressourcen resultieren (Bamberger, Wrona 1996, 386; Hümmer 2001, 50; Al-Laham 2003, 112; Talaulicar 2004, 1644). Dabei ergeben sich Wettbewerbsvorteile nicht aus dem bloßen Vorhandensein der Ressourcen, sondern einerseits aus organisatorischen Fähigkeiten, mittels derer Ressourcen eingesetzt und kombiniert werden und andererseits aus dem Aufbau und der Verteidigung einzigartiger Ressourcen (Grant 1991, 122; 2001, 118). Um zum Aufbau und zur dauerhaften Erhaltung von Wettbewerbsvorteilen bzw. zur Begründung überlegener Marktpositionen beizutragen, müssen Ressourcen (1) wertvoll, (2) knapp, (3) nicht bzw. eingeschränkt imitierbar, (4) nicht substituierbar sowie (5) begrenzt abnutzbar, (6) mobil und (7) vielseitig einsetzbar und (8) nicht aneigenbar sein (Prahalad, Hamel 1990, 83ff; Barney 1991, 106f; Grant 1991, 123ff).

(1) Demnach sind Ressourcen dann wertvoll, wenn sie einen Wert für den Kunden schaffen oder zur Verbesserung der Effektivität und Effizienz von Unternehmen beitragen (Barney 1991, 106; Grant 1991, 121). (2) Sie sind dann besonders nachhaltig, wenn sie aufgrund einer begrenzten Verfügbarkeit und eines eingeschränkten Zugangs knapp sind (Barney 1991, 106). (3) Die Nicht-Imitierbarkeit von Ressourcen kann u.a. auf eine unternehmensindividuelle Vergangenheitsentwicklung, kausale Ambiguität, soziale Komplexität, Isolationsmechanismen oder eine Unternehmensspezifität der Ressourcen zurückgeführt werden (Rumelt 1984, 567; Reed, DeFillippi 1990, 91ff; Barney 1991, 107ff; Grant

Sichtweise des Unternehmens als ein System produktiver Ressourcen und hebt die Bedeutung spezifischer Ressourcenkombinationen hervor.

[7] Eine ausführliche Diskussion des Ressourcenbegriffes erfolgt in Abschnitt 2.1.2.

1991, 126). (4) Neben der Nicht-Imitierbarkeit knapper und wertvoller Ressourcen trägt auch deren unvollkommene Substituierbarkeit zur Nachhaltigkeit bei. Ressourcen können durch ähnliche oder auch vollkommen andere Ressourcen substituiert werden und dadurch deren Wert und Knappheit negativ beeinträchtigt werden (Barney 1991, 111f). (5) Die Nachhaltigkeit wird durch die Abnutzung von Ressourcen und den damit verbundenen Wertverlust negativ beeinträchtigt, wobei die Abnutzbarkeit je nach Ressourcentyp variiert (Teece 2002, 15f)[8]. (6) Ressourcen unterscheiden sich auch im Hinblick auf ihre Mobilität bzw. Transferierbarkeit, wobei deren Nachhaltigkeit insbesondere dadurch gefördert wird, dass sie nicht einfach auf Märkten erworben oder zwischen Unternehmen ausgetauscht werden können (Barney 1991, 103). (7) Ressourcen müssen auch in einer Vielzahl an Produkten oder Dienstleistungen bzw. in Märkten eingesetzt werden können, um nachhaltig zu sein. (8) Letztendlich müssen Unternehmen auch in der Lage sein, sich Ressourcen wie Kompetenzen der Mitarbeiter[9] anzueignen bzw. diese zu sichern. Umso mehr der Wertbeitrag der Mitarbeiter direkt identifizierbar ist, desto höher ist deren Verhandlungsmacht und umso schwerer ist es für das Unternehmen, sich die Kompetenzen der Mitarbeiter zu sichern (Dierickx, Cool 1989, 1507ff).

Das strategische Management zielt letztlich auf die Ausschöpfung und Sicherung der Wettbewerbsvorteile, wobei sowohl eine externe Marktpositionierung als auch eine interne Ressourcenbasis zu berücksichtigen sind (Al-Laham 2003, 15). Somit sind die Markt- und Ressourcenorientierung nicht als konkurrierend, sondern vielmehr als komplementäre Sichtweisen zueinander zu verstehen (Zahn et al. 2000, 153).

2.1.2 Begriffsabgrenzungen

Unter Zugrundelegung dieser strategischen Verortung erfolgt im folgenden Abschnitt eine Diskussion des Ressourcenbegriffes unter Abgrenzung von anderen Begriffen. Eine Abgrenzung der Begrifflichkeiten im Themenumfeld der immateriellen, also physisch nicht fassbaren, Ressourcen ist erforderlich, da sich verschiedenste betriebswirtschaftliche Disziplinen, wie z.B. Rechnungslegung oder Unternehmensführung, mit dem Einfluss immaterieller Ressourcen auf den Wert oder die Performance des Unternehmens auseinandersetzen und somit Begriffsvielfalt besteht. Zum Teil werden Begriffe wie immaterielle Ressourcen, Vermögenswerte, Assets und intellektuelles Kapital synonym verwendet (Lev 2001, 5; Marr, Gray 2004, 102). In der Volkswirtschaftslehre bezeichnen Ressourcen den Oberbegriff für die Produktionsfaktoren Arbeit, Kapital und Boden. Im ressourcenbasierten Ansatz wird der Ressourcenbegriff enger ausgelegt. Wernerfelt bezeichnet Ressourcen als diejenigen materiellen und immateriellen Werte, die semipermanent an das Unternehmen gebunden sind (Wernerfelt

[8] Siehe hierzu auch Abschnitt 2.2.5.

[9] Aus Gründen der Vereinfachung wird im Folgenden die männliche Form von Mitarbeiter verwendet, wobei sich die Aussagen auf beide Geschlechter beziehen.

1984, 172). Nach Barney (1991, 101) umfasst der Ressourcenbegriff Fähigkeiten, organisatorische Prozesse, Informationen und Wissen, die Unternehmen erzeugen und zur Implementierung von Strategien zur Verbesserung der Effizienz und Effektivität des Unternehmens einsetzen. Demnach kann eine Unterscheidung in immaterielle, materielle und finanzielle Ressourcen vorgenommen werden.
Immaterielle Vermögenswerte stellen einen bilanziellen Ausdruck dar und werden als Ressourcen (im Sinne von wirtschaftlichem Vorteil bzw. Nutzen) definiert, die keine gegenständliche Substanz aufweisen und im Unterschied zu finanziellen Ressourcen nicht monetär sind (Küting, Dürr 2003, 1; Helm, Meiler 2004, 390; Möller 2004, 488; Lev 2005, 299). Abgrenzend zu immateriellen Ressourcen ist der Begriff immaterielle Vermögenswerte selbst vorwiegend durch die Literatur sowie durch Standards zur Rechnungslegung belegt und stellt deren bilanzielle Aktivierungsfähigkeit bzw. Bewertung in den Vordergrund. So sind nach dem International Accounting Standard (IAS) 38 die Tatbestände Identifizierbarkeit, Beherrschung und künftiger wirtschaftlicher Nutzen für die Aktivierbarkeit erforderlich (für Details siehe auch 2.3.3). Der Ansatz des intellektuellen Kapitals fokussiert die Bewertung aller immateriellen Ressourcen eines Unternehmens unabhängig von ihrer Aktivierbarkeit im bilanziellen Verständnis. Intellektuelles Kapital umfasst nach Brooking (1996, 8) die Summe aller immateriellen Ressourcen, die zur Geschäftstätigkeit des Unternehmens beitragen. Edvinsson (1997, 368) subsumiert unter dem Begriff intellektuelles Kapital Wissen, Erfahrungen, Technologien, Kundenbeziehungen und (Mitarbeiter-)Fähigkeiten, die zum Aufbau von Wettbewerbsvorteilen führen. Nach Stewart (Stewart 1997, 9f) umfasst das intellektuelle Kapital immaterielle Werte wie Informationen, Wissen und Erfahrungen, die zur Wertgenerierung eingesetzt werden können[10]. Die Definitionen zum intellektuellen Kapital haben gemein, dass sie den Beitrag immaterieller Ressourcen zur Wertschöpfung bzw. zur Generierung von Wettbewerbsvorteilen in den Vordergrund stellen. Das intellektuelle Eigentum stellt dabei den Teil des intellektuellen Kapitals dar, der rechtlich geschützt (z.B. Patente, Copyrights) werden kann (Sullivan 1999, 133; Contractor 2000, 244f; Lev 2005, 299).
Insgesamt werden Ressourcen im Rahmen der Managementliteratur nach einer ressourcenbasierten Perspektive als Inputs zur Leistungserstellung angesehen und können materieller, immaterieller und finanzieller Natur sein. Die Literatur sowie die entsprechenden Rechnungslegungsstandards zu immateriellen Vermögenswerten fokussieren deren Bilanzierung und diskutieren insbesondere Voraussetzungen für deren Ansetzbarkeit. Der Ansatz des intellektuellen Kapitals stellt einen Sammelbegriff dar und fokussiert die Identifikation von Werttreibern etc. In Bezug auf die nachfolgende Begriffsverwendung wird zwischen Ressourcen und Vermögenswerten unterschieden, wobei sich letztere durch die Aktivierungsfähigkeit nach dem bilanziellen Verständnis abgrenzen und Ressourcen einen Sammelbegriff darstellen. Da die Thematik Wissensrisiko unabhängig von einer bilanziellen Aktivierungsfähigkeit betrachtet wird, wird im Folgenden primär der Begriff Ressourcen verwendet.

[10] Siehe hierzu auch (Deking 2003, 22).

2.1.3 Kategorisierung von Ressourcen

Nach der zuvor dargestellten weiten Auslegung des Ressourcenbegriffs erfolgt in diesem Abschnitt eine Kategorisierung von Ressourcen mit dem Ziel, Gemeinsamkeiten der zum Teil heterogenen Kategorisierungsansätze herauszuarbeiten und somit ein klares Verständnis zu schaffen, das dieser Arbeit zugrunde liegt.

Neben finanziellen Ressourcen, die sowohl in der Managementliteratur als auch in der Literatur zur Rechnungslegung als eigene Kategorie angesehen werden (Küting, Dürr 2003, 1; Helm, Meiler 2004, 390; Möller 2004, 488; Lev 2005, 299), werden materielle und immaterielle[11] Ressourcen unterschieden. Einige Autoren führen personelle Ressourcen als eigene Kategorie auf dieser Aggregationsebene an (Bamberger, Wrona 1996, 387; Grant 2001, 111f). Al Laham (2003, 114) kritisiert dabei die mangelnde Trennschärfe zwischen immateriellen und personellen Ressourcen. Da personelle Ressourcen wie Fähigkeiten, Motivation oder Kompetenzen immaterieller Natur sind, können sie den immateriellen Ressourcen zugeordnet werden. Diese Auffassung vertritt auch Hall (1992, 136ff) und unterscheidet immaterielle Ressourcen in personenunabhängige (z.B. Patente, Copyrights, Verträge) und personengebundene Ressourcen (z.B. Kompetenzen). Somit werden in diesem Kontext personelle Ressourcen als Unterkategorie der immateriellen Ressourcen verstanden und umfassen z.B. Ausbildung, Erfahrungen, Urteilsvermögen und Kompetenzen der Mitarbeiter (Barney 1991, 101).

Diese Unterteilung liegt auch dem Ansatz des intellektuellen Kapitals zugrunde, nach dem Human- und Strukturkapital Hauptkomponenten darstellen (Edvinsson 1997; Stewart 1997). Strukturkapital kann in Kundenkapital, das primär Kundenbeziehungen umfasst, und Organisationskapital unterteilt werden und bleibt der Organisation auch bei Verlassen der Organisationsmitglieder erhalten (Wiig 1997, 401). Das Organisationskapital subsumiert in einer feineren Untergliederung organisatorisch verankerte immaterielle Ressourcen, wie z.B. Prozesse, Routinen, Patente, Software oder dokumentiertes Wissen (Wiig 1997, 401)[12]. Vertreter außerhalb der Forschungsströmung intellektuelles Kapital definieren organisatorische Ressourcen als Teil der immateriellen Ressourcen und subsumieren beispielsweise Kontroll-, Koordinationsfähigkeit, Planungs- oder Vertriebssystem unter diesem Begriff (Barney 1991, 101; von Krogh, Roos 1996, 33; Lev 2005, 300). Jedoch ist der Begriff organisatorische Ressourcen sehr weit gefasst, da sowohl finanzielle als auch materielle und immaterielle Ressourcen als organisatorische Ressourcen angesehen werden können, da sie entweder im Besitz des Unternehmens stehen oder zumindest zum Teil von ihm kontrolliert werden. Aus diesem Grund erscheint der Begriff strukturelle Ressourcen an dieser Stelle präziser (Marr 2004, 4). Während nach der Kategorisierung des intellektuellen Kapitals Kundenbeziehungen in der Form des Kundenkapitals

[11] Erste Erwähnungen zur Bedeutung immaterieller Werte gehen auf Hall (1989) sowie Itami und Roehl (1987) zurück.

[12] Der Ansatz des intellektuellen Kapitals wird nochmals bei der Bewertung immaterieller Ressourcen detaillierter aufgegriffen, siehe dazu Abschnitt 2.3 und das entsprechende Schema in Abb. 7 auf Seite 38.

hervorgehoben werden, betonen einige Autoren die Bedeutung von Beziehungen über die Kategorien hinweg und nehmen daher eine Unterteilung in Human-, Organisations- und Beziehungskapital vor (Marr 2004, 4; Piber 2004, 501; Roos et al. 2004, 130; Mertins et al. 2006, 23; Nemetz 2006, 14). Neben Kundenbeziehungen können auch Beziehungen zu Lieferanten, Partnern oder sonstigen Stakeholdern als Teil der immateriellen Ressourcen gesehen werden. Diese Beziehungen stehen nicht im Besitz des Unternehmens und werden zudem zum Teil durch eine andere Partei kontrolliert (Roos et al. 2004, 130). Barney subsumiert Beziehungen einerseits unter den personellen Ressourcen in der Form von Beziehungen zu Mitarbeitern und ordnet sie andererseits den strukturellen Ressourcen in der Form von Beziehungen zwischen Gruppen innerhalb und außerhalb des Unternehmens zu (Barney 1991, 101).

Sullivan (1999, 133) unterscheidet zwischen Humankapital und intellektuellen Ressourcen, wobei letztere durch den Einsatz von Humankapital generiert wurden (z.B. Prozesse, Dokumente, Pläne etc.) und als Untergruppe das intellektuelle Eigentum (z.B. Patente) enthalten, das rechtlich geschützt werden kann (siehe auch Contractor 2000, 244f). Dabei benötigen immaterielle Ressourcen im Allgemeinen und Humankapital im Speziellen finanzielle und materielle Ressourcen wie Gebäude, Infrastruktur etc., um in Produkte inkorporiert werden zu können (Sullivan 1999, 133f).

Zusätzlich zu den bereits angesprochenen Unterscheidungskriterien Personengebundenheit (z.B. Kompetenzen) und rechtliche Schützbarkeit (z.B. Copyright) zieht Hall (1993, 609) die Dynamik als weitere Klassifizierungsdimension heran. So sind immaterielle Ressourcen wie Patente statisch, während organisatorische Fähigkeiten oder Mitarbeiterkompetenzen als dynamisch angesehen werden.

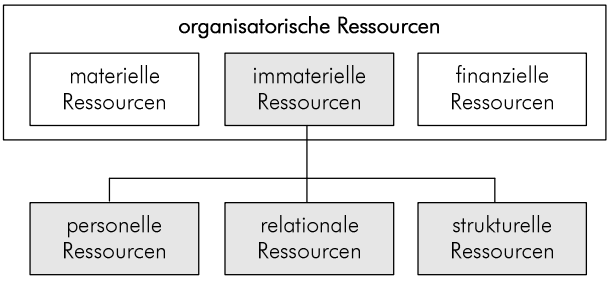


Abb. 3 Kategorisierung von Ressourcen[13]

Die in Abb. 3 dargestellte Kategorisierung von Ressourcen fasst die Ergebnisse der vorangegangenen Diskussion zusammen. Somit können organisatorische Ressourcen in finanzielle, materielle und immaterielle Ressourcen unterteilt werden. Per Definition ist dabei die Trennschärfe gegeben, allerdings bestehen Mischformen zwischen materiellen und immateriellen Ressourcen, die sich durch eine Inkorporierung letzterer ergeben. Die immateriellen Ressourcen können in personelle, relationale und strukturelle Ressourcen unterteilt werden. Personelle Ressourcen umfassen dabei z.B. Fähigkeiten oder Erfahrungen der Mitarbeiter, während relationale Ressourcen Beziehungen zu Kunden, Lieferanten, Partnern und weiteren Stakeholdern einschließen. Letztendlich werden unter der Kategorie strukturelle Ressourcen kulturelle Werte, Prozesse, Routinen und insbesondere auch das intellektuelle Eigentum in der Form von Patenten, Copyrights u.ä. zusammengefasst.

[13] In Anlehnung an (Marr 2004, 4).

2.2 Wissen als zentrale Ressource

Aufgrund verschiedenster interdisziplinärer Sichtweisen besteht hinsichtlich der Konstrukte Wissen und wissensbezogene Ressourcen keine Einigkeit in der wirtschaftswissenschaftlichen Literatur (Maier, 2004, 321). Evident ist jedoch der Wandel zur Wissensgesellschaft, der dazu veranlasst, neuen Triebkräften, Werttreibern und Risiken Beachtung zu schenken. Um eine geeignete Basis für die Analyse von Wissensrisiken zu schaffen, wird in diesem Abschnitt das dieser Arbeit zugrund liegende Begriffsverständnis für Wissen und wissensbezogenen Ressourcen erarbeitet. Dazu wird der Wissensbegriff zunächst in verschiedenen Wissenschaftsdisziplinen, wie z.B. Philosophie und Psychologie, betrachtet, um dann eine Abgrenzung zur betriebswirtschaftlichen Sichtweise vorzunehmen (2.2.1). Auf dieser Basis erfolgt ein knapper Abriss über die Grundzüge des wissensbasierten Ansatzes (2.2.2), der die Verortung des Themengebiets im strategischen Management bzw. in der Unternehmensführung darstellt. Im Anschluss daran werden wissensbezogene Ressourcen und die entsprechenden Wissensträger erörtert (2.2.3), denen im Hinblick auf das Wissensrisikokonzept eine zentrale Bedeutung zukommt, da sich Wissensrisiken primär auf diese Ressourcen auswirken. Die wissensbezogenen Ressourcen lassen sich zudem durch verschiedene Dichotomien charakterisieren, die es bei einer gezielten Steuerung von Risiken in diesem Kontext zu beachten gilt (2.2.4). Analoges gilt für die Besonderheiten immaterieller und im Speziellen wissensbezogener Ressourcen gegenüber materiellen Ressourcen (2.2.5). Der Abschnitt schließt mit der Reflexion von Kriterien, die die Wissensintensität beeinflussen, da eine Steuerung von Wissensrisiken insbesondere für Unternehmen relevant ist, die als wissensintensiv zu charakterisieren sind (2.2.6).

2.2.1 Perspektiven auf Wissen

Der Begriff Wissen wird in verschiedenen Wissenschaftsdisziplinen wie Philosophie, Psychologie, Soziologie, Informatik und Wirtschaftswissenschaften diskutiert, wobei bisweilen kein interdisziplinärer konsensfähiger Bergriff besteht (Roehl 2000, 14; Al-Laham 2003, 23), was zu einem großen Teil auch auf das unterschiedliche Erkenntnisinteresse der verschiedenen Wissenschaftsdisziplinen zurückzuführen ist. In der Philosophie wird der Wissensbegriff als „justified true belief“, also als begründete wahre Überzeugung bezeichnet. Wissen unterscheidet sich demnach von bloßen Meinungen oder subjektiven Überzeugungen dadurch, dass es den Tatsachen entsprechen muss, wobei es nicht ausreicht, dass die Überzeugung zufällig wahr ist, sondern vielmehr eine Begründung erforderlich ist (Güldenberg 1997, 158; Al-Laham 2003, 24). Im Kontext von Unternehmen und Organisationen kommt der Begründung der Überzeugung, die vielfach durch eine intersubjektive Bewährung erreicht wird, eine bedeutende Rolle zu. Nonaka et al. kritisieren an der Sichtweise auf Wissen als „justified true belief“, dass diese Betrachtung zu wenig den individuellen Besonderheiten von Menschen gerecht

wird. Wissen muss vielmehr als dynamisch, kontextspezifisch und handlungsbezogen gesehen werden und hat eine subjektive Komponente, die sich im jeweiligen Wertesystem niederschlägt. Somit liegt Wahrheit immer im Auge des Betrachters (Nonaka et al. 2000, 7).

Neben der Philosophie wird der Wissensbegriff in anderen Wissenschaftsdisziplinen mit jeweils unterschiedlichen Schwerpunktsetzungen diskutiert. So wird beispielsweise in der Psychologie der Begriff Wissen im Zusammenhang mit der Erforschung des menschlichen Denkens, Fühlens und Handelns erörtert. Zentrale Fragestellungen betreffen z.B. die Anwendung von Wissen in Bezug auf Handlungen, die Wissensrepräsentation oder dessen Abhängigkeit vom kulturellen Kontext (Schüppel 1996, 55). Bei einer soziologischen Betrachtung wird Wissen als ein individuelles Konstrukt betrachtet, das von sozialen Kontexten beeinflusst wird (Al-Laham 2003, 24). Aus betriebswirtschaftlicher Perspektive ist es bei der Betrachtung des Wissensbegriffs der Unternehmenskontext besonders relevant. Dabei ist die Übertragbarkeit des Wissensbegriffs aus anderen Wissenschaftsdisziplinen nur schwer möglich, da das Erkenntnisinteresse unterschiedlich ist und dieses die Semantik und Sinnhaftigkeit des verwendeten Wissensbegriffs bestimmt (Romhardt 1998, 25). Somit ist für die Betriebswirtschaftslehre ein eigener Wissensbegriff erforderlich, um die korrespondierenden Fragestellungen trennscharf beantworten zu können (Romhardt 1998, 25).

Auch innerhalb der Wirtschaftswissenschaften, die Wissen im Kontext von Unternehmen und Organisationen betrachten, besteht eine heterogene Auffassung in Bezug auf den Begriff Wissen (Maier et al. 2005, 4). Diese werden nachfolgend erörtert, wobei zunächst eine Abgrenzung von den Begriffen Daten und Informationen erfolgt, um hinreichende begriffliche Trennschärfe zu gewährleisten.

Nach dem Modell der Semiotik wird die Sprache in eine syntaktische, semantische und pragmatische Ebene unterteilt. Erst genannte Ebene fokussiert auf die Beziehung zwischen den Zeichen, während die semantische Ebene die Bedeutung der Zeichen vordergründig betrachtet und Gegenstand der pragmatischen Ebene die Verwendung der Zeichen ist (Lehner et al. 1995, 222f).

Daten entstehen nach dieser Unterscheidung durch die Anordnung und Kodierung von Zeichen mittels syntaktischer Vorschriften und können beispielsweise als Zahlen, Text oder Bilder repräsentiert werden (Lehner et al. 1995, 14). Informationen entstehen durch die Einordnung der Daten in einen Kontext, wodurch sie für den Empfänger an Bedeutung gewinnen und Sinn stiften (Rehäuser, Krcmar 1996, 4; Davenport, Prusak 1998, 4). Die Vernetzung von Informationen, die Denkprozesse wie Verstehen, Verarbeiten und Bewerten bzw. die laufende Interpretation erfordert, ermöglicht die Umsetzung in einem Handlungsfeld (Romhardt 1998, 63; Gabriel, Dittmar 2001, 19)[14]. Auch Sveiby bezeichnet Wissen als Fähigkeit zu handeln (Sveiby 1997, 37). Entlang der Ebenen des Modells der Se-

[14] Die Handlungsorientierung geht bereits auf das altgriechische Wissensverständnis nach Aristoteles zurück. Dieser weist auf die Existenz von Techne hin, wobei es sich um fähigkeitsbasiertes technisches oder handlungsorientiertes Wissen handelt (Schwartz 2006, 17).

miotik erfolgt somit eine Bedeutungsanreicherung (Gemmerich, Stratmann 1998, 24)[15]. Von Wissen ist also erst dann zu sprechen, wenn sich das Handlungspotential eines Individuums oder einer Organisation erhöht hat und dadurch Aufgaben sowie Probleme gelöst werden können (Müller-Stewens, Osterloh 1996, 18). Somit kann nach dieser Sichtweise Wissen als Information in einem bestimmten Kontext gesehen werden, durch den es Personen möglich ist, Informationen zu interpretieren oder bestimmte Handlungen vorzunehmen (Maier 2004, 68f; Müller 2006, 5).

Unter Zugrundelegung dieser Abgrenzung, bestehen im betriebswirtschaftlichen Kontext verschiedene Sichtweisen auf Wissen, die nachfolgend erörtert werden und zur Bildung des der Arbeit zugrunde liegende Begriffsverständnisses herangezogen werden.

- **entscheidungsorientierte Sichtweise:** Im Kontext von Entscheidungen bildet Wissen zum einen die Grundlage auf der Entscheidungen getroffen werden und stellt zum anderen deren Ergebnis dar (Al-Laham 2003, 25). Der Einfluss von Wissen und Informationen auf Entscheidungen wird in der betriebswirtschaftlichen Forschung thematisiert, wobei die Rationalität von Entscheidungen durch die Unvollständigkeit von Wissen, Schwierigkeiten in Bezug auf die Bewertung zukünftiger Ereignisse, eine begrenzte Auswahl an Entscheidungsalternativen oder auch ein Zuviel an Informationen oder Wissen eingeschränkt wird. Letztgenannter Zustand wird auch „Information Overload“ genannt und ist dadurch gekennzeichnet, dass eine Person aufgrund der Informationsmenge nicht mehr in der Lage ist, die eingehenden Informationen sinnvoll zu nutzen, was zu einer Abnahme der Entscheidungsqualität führt (Probst et al. 2000, 22).
- **lernorientierte Sichtweise:** In einer weiteren betriebswirtschaftlichen Forschungsströmung wird Wissen als Ergebnis von Lernprozessen betrachtet. So wie sich Individuen an Veränderungen durch die Reflexion ihrer Denk- und Handlungsmuster anpassen, passen sich auch Organisationen auf einer aggregierten Ebene an[16]. In diesem Kontext werden Theorien zum organisatorischen Lernen und zur lernenden Organisation interdisziplinär in der Literatur diskutiert. Organisationales Lernen kann in diesem Zusammenhang als Prozess des Wissenserwerbes verstanden werden. Dabei betreffen diese Lernprozesse verschiedene Ebenen im Unternehmen (z.B. Teams, Abteilungen), wobei Lernen auf der individuellen Ebene stattfindet und erst durch die Übertragung auf andere Organisationsmitglieder von organisationalem Lernen gesprochen wird (Lehner 2000, 179; Al-Laham 2003, 25)[17].

[15] Diese Abgrenzung unterliegt jedoch einer gewissen Subjektivität, da die Relevanz und Interpretierbarkeit von Informationen durch das bestehende Wissen beeinflusst wird. Fehlt das entsprechende Vorwissen, so ist die Konversion der Informationen zu Wissen erschwert (Bhatt 2001, 69f).

[16] Siehe hierzu auch (Senge 1990; Garvin 1993).

[17] Zentrale Vertreter sind in diesem Zusammenhang Argyris und Schön, die erstmals organisatorische Lernprozesse im Sinne der Veränderung kollektiver Handlungstheorien, das heißt gemeinsame Leitbilder, an denen die Organisationsmitglieder ihr Handeln orientieren, betrachten (Argyris, Schön 1978).

- **wertschöpfungsfokussierte Sichtweise**: Als weiterer Betrachtungsgegenstand wird der Wertschöpfungsbezug und somit auch der Beitrag zum Unternehmenserfolg herangezogen. Als Konsequenz wird Wissen einerseits als Ressource bzw. Inputfaktor und andererseits als Produkt bzw. Outputfaktor gesehen (Nonaka et al. 2000, 21). So stellt die Ressource Wissen in verschiedenen Ausprägungen wie Kompetenzen, Patenten, Prozessbeschreibungen oder dokumentierten Erfahrungen einen Inputfaktor im Hinblick auf die Generierung der Wertschöpfung dar. Nach dem wissensbasierten Ansatz begründet die Ressource Wissen Wettbewerbsvorteile. Neben der Sichtweise als Inputfaktor wird Wissen auch als Outputfaktor gesehen. Wissen kann somit ein Produkt darstellen, das als Ergebnis unternehmerischer Wertschöpfung auf Märkten verkauft wird. So werden z.B. von Beratungsunternehmen Konzepte, von IT-Unternehmen Software entwickelt oder von Unternehmen, die eigene Forschung betreiben, Patente oder Lizenzen generiert, die weiterverkauft werden. Wissen als Produkt wird ver- bzw. gekauft, wobei menschliches Handeln und die Integration in die Wissensbasis erforderlich sind, damit das Potential derartiger Produkte ausgeschöpft werden kann (Probst et al. 1998, 168ff; Glazer 1999, 59ff).

Im Kontext der betriebswirtschaftlichen Perspektiven auf Wissen wird im Folgenden die wertschöpfungsfokussierte Sichtweise zugrunde gelegt, da durch die Auffassung von Wissen als Input- bzw. Outputfaktor die für die Wissensrisikobetrachtung erforderliche Formalisierung erreicht werden kann.

2.2.2 Grundzüge des wissensbasierten Ansatzes

Die gestiegene wirtschaftliche Bedeutung der Ressource Wissen, die sich in einer erhöhten Wissensintensität von Produkten und Dienstleistungen niederschlägt, wird auch durch die zunehmende Tertiarisierung und die wachsende Anzahl von Netzwerkorganisationen deutlich (Ganz, Hermann 2000, 111; Clarke 2001, 190). Mit diesem Wandel sind eine Reihe von Herausforderungen verbunden, die schon früh in der wirtschaftswissenschaftlichen Forschung erkannt bzw. prognostiziert wurden und die letztendlich unter Einbezug von verschiedensten, teils interdisziplinärer Ideen zum wissensbasierten Ansatz als ein neues Paradigma des strategischen Managements führten. So setzten sich die Ökonomen Solow (1957) und Arrow (1962) mit Lernkurveneffekten auseinander, was eine Erhöhung der Aufmerksamkeit für die Ressource Wissen zur Folge hatte. 1958 sensibilisierte der Philosoph Polanyi (1958) für die Bedeutung des impliziten Wissens, was auch in der wirtschaftswissenschaftlichen Forschung Beachtung fand. Drucker setzte sich bereits in den 50’er und 60’er Jahren mit den Begriffen Wissensarbeit und Wissensgesellschaft auseinander und bezeichnete Wissen als Ressource (Drucker 1959a; 1969). 1976 analysierte Teece die Charakteristika des Technologietransfer und somit auch den Wissenstransfer in multinationalen Unternehmen (Teece 1976). Machlup war der erste Ökonom, der Wissen und verbundene Gebiete volkswirtschaftlich analysierte (Machlup 1980). Nonaka publizierte

(1991) in der Harvard Business Review den Artikel „The knowledge creating company“, was zu einer weiteren Sensibilisierung für die Bedeutung der Ressource Wissen führte.

Der in Abschnitt 2.1.1 dargestellte ressourcenbasierte Ansatz (Wernerfelt 1984; Barney 1991), in dem Wissen als immaterielle Ressource bereits berücksichtigt wurde, stellt für diese Einzelaspekte eine konzeptionelle Wurzel dar. Al Laham (2003, 132ff) identifizierte verschiedene Strömungen wissensbasierter Arbeiten, die entweder den Beitrag der Ressource Wissen, von Kernkompetenzen oder Lernprozessen zur Begründung von Wettbewerbsvorteilen zu erklären versuchen oder sich auf die Erklärung der Existenz und Grenzen der Unternehmung abstellen. Letztgenanntes Ziel beansprucht auch die Theorie der Firma für sich, durch die erklärt werden soll, warum Unternehmen existieren und wodurch deren Größe und Ausrichtung determiniert wird (Coase 1937). So wird die Existenz eines Unternehmens beispielsweise damit begründet, dass sich gegenüber Marktverträgen Performanceverbesserungen (z.B. aus der Integration) realisieren lassen (Connor, Prahalad 1996, 480). Derartige Fragestellungen versuchten Grant und Spender im Rahmen ihrer Arbeiten auf die Ressource Wissen zu adaptieren und zu beantworten und eine wissensbasierte Theorie der Firma zu entwickeln (Grant 1996a; 1996b; Spender, Grant 1996). Sie gehen dabei der Frage nach, welchen Beitrag unternehmensspezifisches Wissen zur Begründung von Wettbewerbsvorteilen leistet und welche Konsequenzen sich daraus für das strategische Management ergeben (z.B. in Bezug auf die Koordination, die Struktur und die Grenzen des Unternehmens). Dabei erhebt Grant nicht den Anspruch, dass der wissensbasierte Ansatz eine Theorie der Firma darstellt, die zum Ziel hat, Strukturen und Verhalten von Wirtschaftsunternehmen zu beschreiben, zu erklären und vorherzusagen, da nicht ausreichend Konsens besteht (Grant 1996a, 110). Dieser mangelnde Konsens liegt nach Foss (2005, 81) an der Vielzahl interdisziplinärer Perspektiven, die Einfluss auf den Ansatz genommen haben.

Abgrenzend zur frühen Theorie der Firma, die Unternehmen als ein Bündel von Produktionsressourcen ansieht, betrachtet Williamson (1990, 8) Unternehmen als Steuerungseinheit oder als Netzwerk aus Verträgen, das die eingehenden Faktoren zusammenführt, synthetisiert und in Produkte und Dienstleistungen überführt. In diese Richtung geht auch die Sichtweise von Spender, nach der die Inkorporierung von Wissen in Produkte und Dienstleistungen eine exponierte Rolle einnimmt. Unternehmen können als dauerhafte Beziehungen zwischen wissensgenerierenden Einheiten wie Individuen, Teams und anderen Unternehmen gesehen werden, denen materielle Ressourcen untergeordnet werden (Spender 1996, 47). Ein Unternehmen kann somit als ein dynamisches, sich entwickelndes und quasiautonomes System der Wissensgenerierung und -anwendung angesehen werden (Spender 1996, 59).

Das Ziel des Unternehmens ist darin zu sehen, verteiltes und verschiedenartiges Wissen in Produkte und Dienstleistungen zu inkorporieren (Grant 1996b, 375; Clarke 2001, 189). Demzufolge kommt dem Unternehmen die Aufgabe zu, die Erstellung und die kommerzielle Nutzung von werthaltigem

Wissen zu steuern (Liebeskind 1997, 624). Zur Erreichung dieses Ziels kommt dem Unternehmen die Aufgabe zu, die Spezialisierung für Mitarbeiter zu ermöglichen und zu erhalten, das spezialisierte Wissen der Mitarbeiter zu koordinieren bzw. zu integrieren und diese Inputs in Outputs zu transformieren (Grant 1997, 451). Aus diesem Grund sieht Lev die organisatorische Infrastruktur, die verschiedene Ressourcen so bündelt, dass sie Wert generieren, als bedeutendste immaterielle Ressource (Lev 2004a, 8f).

Neben der Integration von internem Wissen ist auch der Zugang zu externem Wissen, der z.B. im Rahmen von Kooperationen mittels Partizipation in Netzwerken oder durch Akquisitionen realisiert werden kann, durch das Unternehmen zu steuern, da das erforderliche Wissen aus Zeit- und Kostengründen oftmals nicht intern generiert werden kann (Baughn et al. 1997, 103; Das, Teng 1999, 55; Marsh, Ranft 1999, 44; Teece 2000b, 138; Song et al. 2003, 351). Ein Vorteil der gezielten Integration externen Wissens durch Kooperationen besteht darin, dass ein breiteres Set an Produkt- und Wissenskombinationen möglich wird (Grant 1996b, 383).

Insgesamt wird im wissensbasierten Ansatz Wissen als die bedeutendste strategische Ressource gesehen, durch deren gezielten Einsatz Wettbewerbsvorteile erzielt werden können (Grant 1996b, 375; von Krogh, Roos 1996, 32). Diese sind primär auf das Eigentum über Wissen sowie dessen Generierung, Anwendung, Schutz sowie Transfer bzw. Replikation zurückzuführen, wobei diese Prozesse durch das Unternehmen unterstützt werden können (Kogut, Zander 1992, 384; Almeida et al. 2002, 149; Teece 2002, 29; Carrión et al. 2004, 132; Szulanski, Jensen 2004, 348). Leistungsdifferenzen oder Performanceunterschiede zwischen Unternehmen werden im wissensbasierten Ansatz somit u.a. durch unterschiedliche Wissensbasen und Lernkompetenzen erklärt (Zahn et al. 2000, 262). Da die Verbreitung idiosynkratischer Ressourcen die darauf basierenden Wettbewerbsvorteile negativ beeinträchtigen kann, muss neben der Replikation von Wissen auch dessen Imitation durch Dritte geschützt werden (Grant 1997, 452; Matusik 2002b, 608). Nachdem der wissensbasierte Ansatz als strategischer Rahmen dargestellt wurde, werden nachfolgend wissensbezogene Ressourcen, die die zentralen Werttreiber darstellen, näher betrachtet.

2.2.3 Wissensbezogene Ressourcen und Wissensträger

Im Rahmen dieses Abschnitts wird zuerst eine Begriffsabgrenzung in Bezug auf wissensbezogene Ressourcen vorgenommen. Im Anschluss daran werden verschiedene Träger, an die Wissen gebunden ist, betrachtet und auf dieser Basis eine Systematisierung wissensbezogener Ressourcen vorgenommen. Die zum Teil sehr heterogene Auffassung des Ressourcen- und Wissensbegriffs in der betriebswirtschaftlichen Literatur (siehe 2.2.1) setzt sich auch bei der heterogenen Betrachtung von wissensbezogenen Ressourcen, die auf Wissen basieren und im Folgenden als wissensbezogene Ressourcen bezeichnet werden, fort. Ausgehend von dem in den Abschnitten 2.1.2 und 2.1.3 dargelegten Grund-

verständnis zu Ressourcen stellen wissensbezogene Ressourcen eine Unterkategorie der immateriellen Ressourcen dar (Teece 2002, 15; Helm, Meiler 2004, 389). Wie bei Ressourcen im Allgemeinen, ist es auch bei wissensbezogenen Ressourcen im Speziellen nicht ausreichend, dass Unternehmen über diese verfügen, da der Wertbeitrag vorwiegend aus der Bündelung resultiert (Hümmer 2001, 52; DeNisi et al. 2003, 9). Um unternehmensspezifische Ressourcen gezielt steuern zu können, muss eine Konzentration auf diejenigen Ressourcen erfolgen, die eine strategische Relevanz aufweisen bzw. wertvoll oder Wert generierend sind. Davon ist dann auszugehen, wenn diese Ressourcen zur Erstellung von Produkten oder zur Erzielung des Unternehmenserfolgs wesentlich beitragen (Zack 1999, 46ff; Civi 2000, 168; Rodgers 2003, 181; Carlucci, Schiuma 2006, 38). Die Bestimmung des Beitrags wissensbezogener Ressourcen zur Erstellung von Produkten und Dienstleistungen wird auch im Rahmen von Intellectual Capital Reports thematisiert, die im Zusammenhang mit der freiwilligen Berichterstattung (siehe 2.3.3) relevant sind (Mourtisen 2005, 213). Zusammenfassend werden wissensbezogene Ressourcen als eine Unterkategorie immaterieller Ressourcen aufgefasst, die zu einem erheblichen Teil auf Wissen basieren, strategisch bedeutend sind und zur Erstellung von Produkten bzw. zur Erreichung der Unternehmensziele wesentlich beitragen.

Wissensbezogene Ressourcen können in Unternehmen in vielfältiger Weise auftreten und von Mitarbeiterkompetenzen, Ideen der Mitarbeiter über Lessons Learned bis hin zu Patenten reichen. Dabei wird von einigen Autoren hervorgehoben, dass Wissen einen physischen Träger erfordert, um als Ressource bzw. Inputfaktor eingesetzt werden zu können (Rehäuser, Krcmar 1996, 16; Amelingmeyer 2002, 52). Amelingmeyer subsumiert unter dem Begriff Wissensträger diejenigen körperlichen Elemente, in denen sich Wissen manifestieren kann (Amelingmeyer 2002, 52). Jedoch besteht in diesem Zusammenhang eine heterogene Auffassung darüber, inwiefern Wissen losgelöst von Personen an nicht-menschliche Wissensträger gebunden sein kann. DeNisi et al. sehen wissensbezogene Ressourcen als eine Untergruppe des Humankapitals und fokussieren demnach auf Personen als ausschließliche Wissensträger (DeNisi et al. 2003, 6). Auch Müller (Müller 2006, 5) vertritt die Ansicht, dass Wissen immer an Personen gebunden ist. Bach und Homp (1997, 5) erweitern dieses Verständnis von Wissensträgern ausgehend vom Individuum auf verschiedenste Gruppen wie Organisationseinheiten oder Netzwerke, an die Wissen gebunden ist. Nach dieser Auffassung kann Wissen auf mehrere Personen verteilt und somit organisatorisch verankert sein. Verschiedene Autoren gehen noch einen Schritt weiter und beziehen nicht-menschliche Wissensträger, wie z.B. Dokumente oder Datenbanken, mit ein (Walsh, Ungson 1991, 59; Rehäuser, Krcmar 1996, 16; Güldenberg 1997, 267; Zack 1999, 46; Ford 2001, 561; Zins 2006, 449). Dieser Dualität trägt auch die Sichtweise von Zack Rechnung, der

Wissen sowohl als Objekt, das gespeichert und manipuliert werden kann als auch als Prozess des gleichzeitigen Wissens und Handelns sieht (Zack 1999, 46)[18].

Al Laham hebt hervor, dass in den jüngeren Beiträgen zum WM übereinstimmend die Auffassung vertreten wird, dass auch dokumentiertes explizites Wissen als eine sinnvolle, kontextgebundene Vernetzung von Informationen losgelöst von Personen sein kann (Al-Laham 2003, 34f). Somit stellen auch materielle Objekte Wissensträger dar. Basierend auf diesen Ausführungen kann Wissen neben Personen auch in sozialen Systemen bzw. der Organisation verankert und in Objekten inkorporiert sein. Diese drei Wissensträger werden nachfolgend genauer erläutert.

Person: Aufgrund des starken Personenbezugs von Wissen ist unstrittig, dass die Mitarbeiter als primäre Wissensträger gesehen werden (Strassmann 1998, 3ff; Amelingmeyer 2002, 55). Personelle Wissensträger treten in Unternehmen als eigene Mitarbeiter, Mitarbeiter von Fremdfirmen oder Selbständige auf (Amelingmeyer 2002, 56). Diese stellen dem Unternehmen sowohl Kompetenzen, die in Fach-, Methoden-, Sozial- und Selbstkompetenz unterschieden werden können, als auch Erfahrungen zur Verfügung. Dabei beziehen sich Fachkompetenzen auf Kenntnisse im Tätigkeitsfeld, während sich methodische Kompetenz auf die Anwendung von Systemen, Instrumenten und Methoden bezieht. Soziale Kompetenzen bezeichnen Fähigkeiten im Umgang mit anderen und Selbstkompetenzen Fähigkeiten zur Selbststeuerung (Anwander 2002, 238). Erfahrungen, die im Rahmen der Aufgabenerfüllung gesammelt und mit anderen Mitarbeitern geteilt werden, stellen wertvolle personengebundene wissensbezogene Ressourcen für Unternehmen dar (Blackler 1995, 1024; Strassmann 1998, 4; Nonaka et al. 2000, 21). Mitarbeiter als Wissensträger verkörpern die gesamte Spannweite des Wissens (Amelingmeyer 2002, 54). Diese Spannweite ist im Vergleich zu anderen Wissensträgern größer und ergibt sich daraus, dass Personen mithilfe von Kommunikation nicht ihr gesamtes Wissen anderen Personen zugänglich machen können, da ihnen ihr Wissen zum Teil nicht bewusst ist (Güldenberg 1997, 268f; Ford 2001, 561). Besondere Bedeutung wird in diesem Zusammenhang kognitiven Gedächtnisstrukturen bzw. mentalen Modellen beigemessen. Letztere stellen relativ stabile kognitive Muster räumlicher und zeitlicher Ordnung dar, mit deren Hilfe Personen Wissen aufbewahren und zur Verfügung halten (Amelingmeyer 2002, 54). Ein weiteres Charakteristikum personeller Wissensträger ist deren Potential neues Wissen zu erlernen und aufzunehmen, d.h. neue Informationen anzupassen und zu verarbeiten (DeNisi et al. 2003, 9). So kann es sich bei personenbezogenem Wissen beispielsweise um kognitive Fähigkeiten handeln, die es einer Person ermöglichen, übergeordnete Muster oder komplizierte Zusammenhänge zu erkennen sowie Basisannahmen zu überdenken (Blackler 1995, 1023). Liman betont in diesem Kontext die Fähigkeit, vorhandenes Wissen kombiniert anzuwenden (Liman 1999, 121). Weiterhin zeichnen sich personelle Wissensträger dadurch aus, dass sie im Ver-

[18] Auch Hall hat diesen Gedanken bei der Betrachtung immaterieller Ressourcen verfolgt und unterscheidet zwischen statischem objektbezogenen und dynamischem personen- bzw. prozessbezogenen Wissen (Hall 1993, 609).

gleich zu anderen Wissensträgern über Übersetzungs-, Ergänzungs-, Kontroll- und Korrekturwissen verfügen (Amelingmeyer 2002, 55f). Personen können ihr Wissen auf andere Personen durch persönliche Gespräche, Präsentationen etc. übertragen (Güldenberg 1997, 268; Amelingmeyer 2002, 56). In diesem Zusammenhang wird auch von kollektiven Wissensträgern gesprochen, die nachfolgend betrachtet werden.

Organisation: Nach Bach und Homp (1997, 5) sind neben einzelnen Mitarbeitern auch organisatorische Einheiten, wie z.B. Teams, Abteilungen, die Gesamtorganisation, unternehmensübergreifende Netzwerke sowie die Gesamtheit der Anspruchsgruppen, so genannte kollektive Wissensträger[19]. Nach Amelingmeyer (2004, 68) kann zudem zwischen formellen und informellen kollektiven Wissensträgern unterschieden werden, wobei erstere in der Organisation explizit vorgesehen sind, während informelle kollektive Wissensträger eher ungeplant und zufällig auftreten[20]. Wissen kann in diesem Zusammenhang sowohl auf mehrere Personen verteilt sein als auch nur im Kollektiv bestehen (Ford 2001, 561). Das Gruppenwissen entsteht somit aus der Kombination von Spezialwissen, über das die einzelnen Gruppenmitglieder verfügen und das von ihnen eingebracht wird. Das Wissen einer Gruppe ist ferner dadurch gekennzeichnet, dass es mehr Wissen als die Summe des Wissens der einzelnen Mitglieder umfasst (Ford 2001, 561; Amelingmeyer 2004, 67). Die Forschungsansätze zum Gruppengedächtnis können zum Verständnis dieses Phänomens eine Erklärungshilfe geben. Bedingt durch die Verteilung des Wissens auf mehrere Mitglieder und die wechselseitige Nutzung sind in bestimmten Fällen nur alle Gruppenmitglieder gemeinsam in der Lage, sich zu erinnern (Oberschulte 1996, 571). Nach Wegner kann eine Unterteilung zwischen individuellem und externem Gedächtnis vorgenommen werden, wobei ersteres das Gedächtnis eines einzelnen Individuums betrifft, während verschiedene externe Speicher, wie z.B. Bücher oder elektronische Aufzeichnungen, das externe Gedächtnis bilden. Im individuellen Gedächtnis sind die entsprechenden Speicherpfade abgelegt. Neben diesen externen Speichern werden auch Personen in analoger Weise als Speicher genutzt. Wegner bezeichnet dies als transaktives Gedächtnis, das sich aus einer Menge von individuellen Gedächtnissystemen sowie der Kommunikation zwischen diesen Personen zusammensetzt. Auch in diesem Fall wird der Zugriffspfad zum Wissen der anderen Personen im individuellen Gedächtnis gespeichert (Wegner 1986, 186ff). Neben der komplementären Verteilung von Gruppenwissen ist Wissen auch redundant auf mehrere Organisationsmitglieder verteilt. Dies wird z.B. dadurch nachvollziehbar, dass Aufgaben bzw. Prozesse, die von bestimmten Mitarbeitern langjährig bearbeitet wurden, teilweise zeitnah durch Nachfolger ausgeführt werden können. Dies ist darauf zurückzuführen, dass das zur Ausführung der Aufgaben erforderliche Wissen verteilt bei anderen Mitarbeitern der Organisations-

[19] Wissen wird in diesem Zusammenhang als komplexes soziales Phänomen gesehen, das in verteilten Aktivitätssystemen auftritt (Lave 1993, 8).

[20] Als Beispiel können in diesem Kontext informelle Communities im Unternehmen angeführt werden, die sich aus dem Interesse an einem bestimmten Thema ergeben.

einheit vorhanden ist und durch diese weitergegeben wird. Auf mehrere Personen verteiltes bzw. von diesen geteiltes Wissen zeigt sich auch in einem gemeinsamen Verständnis oder in einer gemeinsamer Sprache (Blackler 1995, 1024), die ihrerseits wiederum eine bedeutende wissensbezogene Ressource darstellen können.

Wegner nimmt in diesem Kontext eine feinere Unterteilung vor und unterscheidet zwischen integriertem und differenziertem transaktiven Gedächtnis. In einem integrierten transaktiven Gedächtnis werden identische Informationen in mehreren verschiedenen Gedächtnissen abgelegt, während differenzierte transaktive Gedächtnisse dadurch gekennzeichnet sind, dass die jeweilige Information nicht redundant gespeichert, sondern nur in jeweils einem Gedächtnissystem vorhanden ist (Wegner 1986, 204).

Neben der Verteilung von Wissen auf mehrere Personen wird an Personen gebundenes Wissen durch die Anwendung in Geschäftsprozessen bzw. die regelmäßige Anwendung durch die Mitarbeiter im Zeitverlauf in Prozessen, Routinen und Strukturen organisatorisch verankert (Walsh, Ungson 1991, 59; Starbuck 1992, 720f; North 1999, 27; Tsoukas, Vladimirou 2001, 976; Cummings 2003, 7; Szulanski, Jensen 2004, 348). Dabei führt die Anwendung des Wissens im Tagesgeschäft zu Denk- und Handlungsmustern, die von mehreren Organisationsmitgliedern geteilt werden. Die permanente Anwendung bedingt eine Verankerung und Generalisierung dieser Muster, die dann als organisatorische Routinen bezeichnet werden können (Nonaka et al. 2000, 22; Tsoukas, Vladimirou 2001, 976). Raub und Büchel bezeichnen organisationale Routinen als die Integration individueller Fähigkeiten in den Rahmen komplexer organisationaler Abläufe. Sie speichern das organisationale Wissen bezüglich einer bestimmten Problemlösung (Raub, Büchel 1996, 27; Güldenberg 1997, 279).

Auch Blackler weist auf die Inkorporierung von Wissen in Routinen hin, die als komplexer Mix interpersoneller, technologischer und sozio-struktureller Faktoren gesehen werden können (Blackler 1995, 1023f). Gerade diese Routinen und Prozesse sind im Hinblick auf die Generierung von Wettbewerbsvorteilen von Bedeutung, da sie verschiedenste organisatorische Ressourcen bündeln und so direkt bzw. indirekt zur Wertschöpfung beitragen (Grant 2001, 118).

Zudem kann, wie bereits erwähnt, Wissen auch losgelöst von Personen in Objekten inkorporiert sein. Im Falle von personenbezogenem Wissen kann dies z.B. durch die Dokumentation von Erfahrungen oder die Erstellung von Konzepten erfolgen. In Bezug auf organisatorisch verankertes Wissen kann diese Loslösung durch Prozessdokumentation erfolgen (Amelingmeyer 2002, 56)[21]. Diese Loslösung von Wissen von Personen ist Gegenstand des nachfolgend thematisierten materiellen Wissensträger. Best Practices stellen in diesem Zusammenhang einen Übergang von organisatorisch verankertem und in Objekten inkorporiertem Wissen dar.

[21] Als Beispiel kann in diesem Zusammenhang die umfassende Dokumentation von Prozesswissen im Franchisebereich (z. B McDonald) angeführt werden, die Wissenstransfer und Standardisierung ermöglicht (Argote, Ingram 2000, 154; Reinhardt 2002, 23).

Objekt: Desouza und Vanapalli (2005, 77) unterscheiden im Hinblick auf die Werthaltigkeit von Wissen zwischen „knowledge routines“ und „knowledge assets“. Erstere betreffen Wissen, das im Rahmen von Prozessen und Routinen inkorporiert ist und im Unternehmen angewandt wird. Neben diesem angewandten Wissen besteht kodifiziertes Wissen, das auch an nicht-menschliche Wissensträger gebunden sein kann. Auch Zack betont diese Dualität, nach der Wissen einerseits als Objekt gespeichert und manipuliert werden und andererseits als Prozess des gleichzeitigen Wissens und Handelns gesehen werden kann (Zack 1999, 46). Somit kann Wissen auch unabhängig von Personen oder Gruppen in Objekten verankert sein. Dabei kann derartiges Wissen einerseits in verschiedensten Formen des intellektuellen Eigentums (z.B. Patente, Marken) des Unternehmens inkorporiert (Sullivan 1999, 133; Contractor 2000, 245; Nonaka et al. 2000, 21f) und andererseits in Produkten verankert sein (Starbuck 1992, 720f; Strassmann 1998, 8f; North 1999, 27; Lev 2005, 200). Pfeiffer (1965, 46ff) unterscheidet bei in Objekten inkorporiertem Wissen noch feiner in materielle (z.B. physische Produkte), quasimaterielle (z.B. elektronisch dokumentiertes Wissen) und rechtliche Wissensträger (z.B. gewerbliche Schutzrechte). Darüber hinaus ist ein Teil des explizierbaren Wissens einer Organisation auch in der Form von Lessons Learned, Schulungsunterlagen oder Projektberichten dokumentiert, wobei im Hinblick auf eine Abgrenzung zu dokumentierten Informationen eine stärkere Kontextualisierung herangezogen wird (Blackler 1995, 1023ff; Nonaka et al. 2000, 21f; Maier et al. 2005, 23).

Materielle Wissensträger können nach Amelingmeyer (2004, 59) in druckbasierte (z.B. Bücher, Fachzeitschriften), audiovisuelle (z.B. Filme, Fotos), computerbasierte (z.B. Festplatten, optische Laufwerke) und produktbasierte (z.B. Fertigungsanlagen, Erzeugnisse) unterschieden werden. Mit deren Einsatz können unterschiedliche Ziele wie Vervielfältigung, Sicherung von Rechten (z.B. Patentschriften), Vermittlung von Wissen an andere Wissensträger (z.B. Lehrmaterial) etc. verfolgt werden (Amelingmeyer 2004, 57). Ein Abgrenzungsmerkmal zu anderen Wissensträgern besteht darin, dass in Objekten inkorporiertes Wissen im Unternehmen auch noch vorhanden ist, wenn Mitarbeiter das Unternehmen verlassen (Blackler 1995, 1023ff). Somit kann derartiges Wissen unabhängig von Personen manipuliert und transferiert werden (Ford 2001, 561).

Im Folgenden wird vielfach auf elektronisch dokumentiertes Wissen Bezug genommen, da dieses aufgrund seiner hohen Verbreitung von besonderer Relevanz für den Untersuchungsgegenstand ist. Bei elektronisch dokumentiertem Wissen handelt es sich bei einer technischen Betrachtung um semistrukturierte Daten, die z.B. in Dokumentenmanagement-, Contentmanagement- oder Mailsystemen in Unternehmen verwaltet werden und im Vergleich zu strukturierten Daten mit einem erhöhten Aufwand für Speicherung, Organisation und v.a. Wiederfinden einhergehen.

Marr, Schiuma und Neely (2004, 562) sehen zudem in der im Unternehmen eingesetzten IKT eine wissensbezogene Ressource, sofern diese auf Wissen basiert und einzigartig ist. Das in IT-Systemen verwaltete bzw. gesicherte Wissen ist im Wesentlichen der Kategorie Objekt zuzuordnen. Dabei sind

Geschäftsprozesse im Allgemeinen sowie Mitarbeiter und organisationale Routinen im Speziellen aufgrund des Wandels zur Wissensgesellschaft von einer IT-Infrastruktur, die Wissen angemessen, qualitativ und zuverlässig verwaltet und bereitstellt, in zunehmendem Maße abhängig (Junginger, Krcmar 2003, 16; Hirschmann, Romeike 2004, 13). Da mittlerweile eine Vielzahl von sensitiven Informationen und Wissenselementen in IT-Systemen verwaltet bzw. gesichert ist, stellen IT-Systeme eine essentielle Ressource dar, die im Rahmen des in Objekten inkorporierten Wissens eines besonderen Schutzes bedarf, um Einschränkungen der Produktivität zu vermeiden und die Wertschöpfung sicherzustellen.

Obwohl Wissen losgelöst von Personen in Objekten inkorporiert sein kann, so ist dennoch menschliches Handeln und die Integration in die Wissensbasis erforderlich, damit das Potential des losgelösten Wissens ausgeschöpft werden kann (Probst et al. 1998, 168ff; Glazer 1999, 59ff). Die verschiedenen Wissensträger werden nochmals in Abb. 4 zusammengefasst.

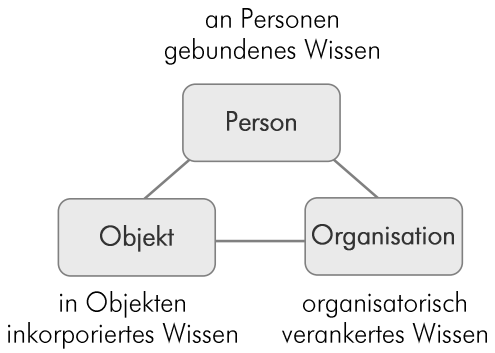


Abb. 4 Unterteilung wissensbezogener Ressourcen

Demnach ist Wissen in der Form von Erfahrungen und Fähigkeiten an die Mitarbeiter gebunden, in Prozessen und Routinen organisatorisch verankert oder auch in Produkten, Dienstleistungen und dokumentiertem (kontextualisierten) Wissen in Objekten inkorporiert. Dabei ist diese Dreiteilung nicht als trennscharf zu verstehen, da auch Kombinationen aus diesen Kategorien auftreten, was insbesondere auch durch den starken Personenbezug von Wissen erklärt werden kann. Insbesondere die Bündelung bzw. Interaktion von einzelnen wissensbezogenen Ressourcen, die an verschiedene Wissensträger gebunden sind, leistet einen Beitrag zur Wertschöpfung bzw. macht die Wettbewerbsvorteile eines Unternehmens erst aus[22]. Marr, Schiuma und Neely (2004, 562) unterteilen explizit wissensbezogene Ressourcen in Aktoren (Stakeholderressourcen) und Infrastruktur (strukturelle Ressourcen), wobei unter erstgenannten sowohl Beziehungen zu Kunden, Lieferanten und Partnern als auch das Humankapital nach dem Verständnis des Ansatzes zum intellektuellen Kapital subsumiert werden. Die Infrastruktur (strukturelles Kapital) wird in eine physische und virtuelle Komponente unterteilt (siehe Abb. 5). Erstere umfasst die IT wie Datenbanken, Server und Netzwerke, die auf spezifischem Wissen basiert und einzigartig ist (Marr et al. 2004, 562). Unter der virtuellen Infrastruktur werden die Kultur des Unternehmens, dessen Prozesse und Routinen sowie dessen intellektuelles Eigentum in der Form von Copyrights, Patenten etc. systematisiert. Bedeutend sind in diesem Zusammenhang die Interaktionen zwischen „denkenden“ Aktoren

[22] Auch Argote und Ingram (2000, 154) thematisieren in diesem Kontext die Interaktion zwischen Wissensträgern.

(Stakeholder Ressourcen) und „nicht denkender“ Infrastruktur (strukturellen Ressourcen), was auch die Dynamik und die starke Personengebundenheit von Wissen hervorhebt (Marr et al. 2004, 563). Auch Sullivan (1999, 133f) betont das Erfordernis einer geeigneten Infrastruktur für die Inkorporierung von Wissen in Produkte. Die Bedeutung der Interaktion zeigt sich beispielsweise darin, dass der Transfer von bestehendem Wissen zum Teil nur dann erfolgreich bzw. effizient ist, wenn mehrere Wissensträger (z.B. Abteilungen) gleichzeitig transferiert werden (Teece 2000a, 36). Ein Beispiel ist die Abwerbung einer gesamten Forschungs- und Entwicklungsabteilung durch Konkurrenten. Da insbesondere durch die Interaktionen zwischen wissensbezogenen Ressourcen bzw. unterschiedlichen Wissensträgern Wert generiert wird, werden sie auch explizit bei der Betrachtung von Wissensrisiken in Kapitel 5 berücksichtigt.

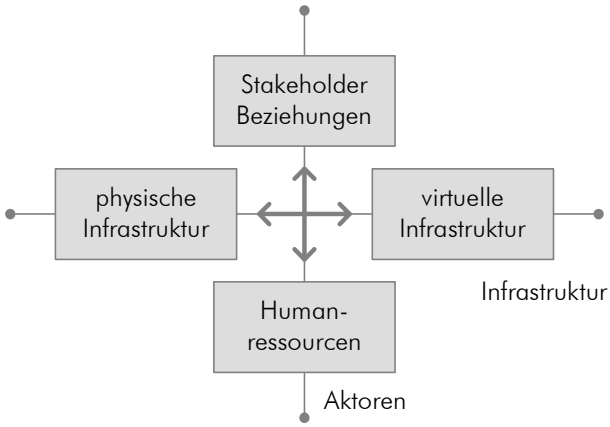


Abb. 5 Interaktion wissensbezogener Ressourcen[23]

2.2.4 Dimensionen zur Spezifizierung wissensbezogener Ressourcen

In der Literatur zum WM hat sich eine Vielzahl von Dichotomien herausgebildet, mittels derer Wissen im Unternehmenskontext genauer beschrieben wird. In diesem Abschnitt werden wissensbezogene Ressourcen zusätzlich zu ihrer Bindung an Wissensträger (siehe 2.2.3) auf der Basis der entsprechenden Dimensionen detailliert betrachtet, um so eine Systematisierungsmöglichkeit zu schaffen. Dabei erfolgt im Rahmen dieses Abschnitts eine Fokussierung auf diejenigen Dichotomien, die für den Untersuchungsgegenstand Wissensrisiko von Relevanz sind[24].

- **Explizierung**: Als weit verbreitete Dichotomie wird zwischen explizitem und implizitem Wissen unterschieden. Erstgenanntes ist artikulierbar, was sich in sprachlicher Umsetzbarkeit äußert. Explizites Wissen ist somit kodifizierbar und im Falle eines menschlichen Wissensträgers auch bewusst. Implizites Wissen wird durch Erfahrung erlernt, ist nicht bewusst und somit vergleichsweise schwer artikulierbar bzw. kodifizierbar (Nonaka, Takeuchi 1995, 73; Matusik, Hill 1998, 683; Argote, Ingram 2000, 158; Amelingmeyer 2002, 47). Vielfach wird zwischen den beiden Polen der Dimensionen zu stark polarisiert, was nicht der ursprünglichen Intention Polanyis entspricht,

[23] Die Abbildung basiert auf (Marr et al. 2004, 562).

[24] Die Relevanzbestimmung erfolgt dabei nicht nach subjektiver Einschätzung, sondern stützt sich auf die Auswahl durch andere Autoren, die sich bereits mit einem ähnlichen Untersuchungsgegenstand befasst haben. Siehe hierzu z.B. (Matusik 2002a).

da er davon ausgeht, dass jedes explizite Wissen einen gewissen impliziten Anteil hat (Polanyi 1966, 24f).

- **Kodifizierung**: Als weitere Dichotomie kann eine Unterscheidung zwischen kodifiziertem und nicht kodifiziertem Wissen vorgenommen werden. Kodifizierung bedeutet in diesem Kontext, dass Wissen losgelöst von Personen in verschiedensten Dokumentationen (z.B. Konzepten, Patenten, Handbüchern) inkorporiert sein kann. Zum Teil erfolgt in diesem Kontext in der Forschung eine Gleichsetzung der Ausprägungen explizit und kodifiziert. Dies trifft allerdings nicht zu, da die Dimension Explizierung primär angibt, inwieweit Wissen bewusst, artikulierbar bzw. vermittelbar ist, was nicht zugleich bedeutet, dass eine Kodifizierung erfolgt ist. Die Kodifizierung von explizitem Wissen ist vergleichsweise einfacher (Zander, Kogut 1995, 77,82).
- **organisatorische Verbreitung**: Wissen kann, wie in Abschnitt 2.2.1 bereits erwähnt, in Unternehmen unterschiedlich weit verbreitet sein. In diesem Kontext wird auch von kollektivem Wissen gesprochen. Individuelles Wissen bezeichnet z.B. Kompetenzen oder Erfahrungen der Mitarbeiter, während Wissen über Produkte, Prozesse, Strategien oder Kultur zumeist von mehreren Mitarbeitern geteilt wird und dementsprechend kollektiviert ist (Matusik, Hill 1998, 683; Ford 2001, 561). In Bezug auf die Verbreitung kann noch eine feinere Unterteilung vorgenommen werden. So kann Wissen von Individuen über Gruppen, Abteilungen, die gesamte Organisation und über die Grenzen der Organisation hinaus geteilt werden (Kogut, Zander 1992, 388)[25].
- **Spezifität**: Als weitere Unterscheidung kann die Spezifität von Wissen angeführt werden. So kann Wissen unternehmensspezifisch sein, was zur Folge hat, dass eine Anwendung außerhalb des Unternehmens nur schwer bzw. gar nicht möglich ist (Child 2001, 661; Jacob, Ebrahimpur 2001, 84). Diese Begrenzung kann sich je nach Spezifität auf Team-, Abteilungs- und Unternehmensgrenzen auswirken und kann die Aufnahme des Wissens insbesondere durch Unternehmensexterne erschweren (Simonin 1999, 600; Parise, Henderson 2001, 911). Auf der anderen Seite kann Wissen eine gewisse Allgemeingültigkeit aufweisen und bedarf somit keines unternehmensspezifischen Kontexts. Allgemeines Wissen kann in verschiedenen Unternehmen in gleicher Weise zum Einsatz kommen. Dies trifft u.a. auf natur- und ingenieurwissenschaftliche Kenntnisse, auf den Umgang mit dem PC o.ä. zu. Demgegenüber stellen Kenntnisse über unternehmensinterne Abläufe, die Bedienung von Spezialmaschinen oder die Anwendung von unternehmensindividuellen Softwaretools Beispiele für spezifisches Wissen dar (Amelingmeyer 2002, 51)
- **Kontexteinbettung**: In Bezug auf die Typisierung von Wissen kann auch der Grad der Einbettung von Wissen bzw. dessen Abhängigkeit von anderem Wissen herangezogen und somit als Dichotomiepaar zwischen autonomem und systemischem Wissen unterschieden werden. Autonomes

[25] Spender verknüpft die Verbreitungsdimension mit dem Grad der Explizierung und unterscheidet vier korrespondierende Wissenstypen. Für weitere Details siehe (Spender 1996, 52).

Wissen bezieht sich in diesem Kontext auf einen Einzelaspekt z.B. eine Routine, ein konkretes Produkt o.ä. Systemisches Wissen hingegen betrifft ein höheres Aggregationsniveau, wie z.B. unternehmensweite Routinen oder Koordinationsschemata. Dessen vollständige Erfassung setzt umfangreiches Wissen voraus (Zander, Kogut 1995, 77,82; Matusik, Hill 1998, 684f). Die Einbettung in anderes Wissen beeinflusst die Herauslösbarkeit des Wissens aus dem Kontext und somit auch die Nutzbarkeit bzw. Verständlichkeit für Dritte, die den jeweiligen Kontext nicht kennen. In Bezug auf den Wissenstransfer wird von der Einbettung der Transfererfolg beeinflusst (Baughn et al. 1997, 107; Cummings, Teng 2003, 44).

- **Reifegrad**: In Unternehmen und Organisationen stellen der Grad der Selbstverpflichtung (Commitment) sowie die Autorisierung durch Führungskräfte (Legitimation) zusammen eine wesentliche Dimension im Prozess der Wissensreifung dar. Wissen lässt sich danach einteilen, wie ausgeprägt die Selbstverpflichtung durch Gruppen, Teams oder Communities bzw. die formale Autorisierung durch Führungskräfte ist. Die Reifung von persönlichen Erfahrungen geht über verschiedene Stufen bis hin zu neu gestalteten Wissensprozessen (Maier, Schmidt 2007, 326ff). Amelingmeyer stellt in diesem Kontext auf die Bewährung des Wissens ab und betont, dass subjektives Wissen einzelfallgebunden ist, während sich objektives Wissen intersubjektiv bewährt hat (Amelingmeyer 2002, 46).
- **Geheimhaltung**: Als weitere Dichotomie kann zwischen privatem und öffentlichem Wissen unterschieden werden. Ersteres ist nur im entsprechenden Unternehmen bzw. im Netzwerk verfügbar, während öffentliches Wissen z.B. in der gesamten Branche oder auch branchenübergreifend vorhanden ist. Im Hinblick auf Wettbewerbsvorteile und die Eigenschaften von Ressourcen ist insbesondere privates Wissen von Relevanz, da es die Kriterien selten bzw. unternehmensspezifisch erfüllt (siehe Abschnitt 2.1.1). Privates Wissen schließt in diesem Zusammenhang beispielsweise einzigartige organisationale Routinen, Prozesse, Dokumente oder Handelsgeheimnisse ein, während öffentliches Wissen diese Zugänglichkeitsbarriere nicht aufweist und somit einem öffentlichen Gut gleichgesetzt werden kann. Beispiele sind Best Practices in Bezug auf Anreizsysteme, Lagerhaltung o.ä. der jeweiligen Branche oder Programmier- oder Anwenderkenntnisse für Standardsoftware (Matusik 2002a, 457f). Im Hinblick auf die Wettbewerbsvorteile können sich diese nur aus privatem und nicht aus öffentlichem Wissen ergeben.

Wissensbezogene Ressourcen sind wie in Abschnitt 2.2.3 dargestellt, an verschiedene Träger gebunden und können zudem anhand verschiedener Dimensionen näher spezifiziert werden. So können z.B. Erfahrungen rein personengebunden sein und somit eine einzige Person als Wissensträger aufweisen oder andererseits mündlich verbreitet oder auch entsprechend dokumentiert sein und somit im letztgenannten Fall zusätzlich in ein Objekt (z.B. Dokument) als materiellen Wissensträger inkorporiert sein. In beiden Fällen kann eine nähere Spezifizierung der wissensbezogenen Ressource anhand der in die-

sem Abschnitt dargestellten Dimensionen erfolgen. Je nachdem wie bewusst oder artikulierbar die Erfahrungen sind, variiert der Grad der Explizierung. Sind die Erfahrungen dokumentiert liegt eine Kodifizierung vor, andernfalls nicht. Persönliche Erfahrungen sind im Hinblick auf die organisatorische Verbreitung zumeist individuell, können jedoch bei einer Teilung mit anderen Mitarbeitern zunehmend kollektiver Natur sein.

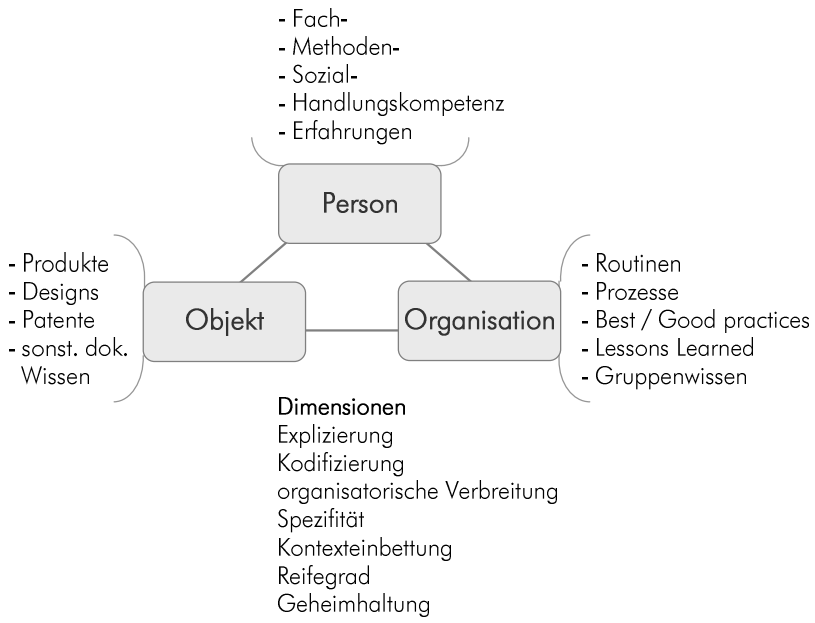


Abb. 6 Beispiele zu wissensbezogenen Ressourcen

Sind diese Erfahrungen dokumentiert, kann sich die organisatorische Verbreitung über die ganze Organisation oder über das Unternehmen hinaus erstrecken. Dabei kommt in diesem Zusammenhang auch der Geheimhaltungsdimension eine besondere Bedeutung zu. So kann im Falle dokumentierten Wissens der Zugriff beschränkt oder im Falle nicht dokumentierten Wissens eine Geheimhaltungsverpflichtung bestehen und somit ein entsprechendes Sicherheitsniveau gegeben sein. Eine weitere Spezifikation kann im Hinblick auf die Unternehmensspezifität der wissensbezogenen Ressourcen erfolgen. So können Erfahrungen beispielsweise allgemeiner Natur sein und die Branche und Themengebiete betreffen oder sich auf unternehmensspezifische Projekte beziehen. Ferner können wissensbezogene Ressourcen in unterschiedlichem Ausmaß in einen Kontext eingebettet sein und anderes Wissen voraussetzen. Hinsichtlich Reifegrad weisen Erfahrungen, solange sie persönlicher Natur sind, von wenigen Mitarbeitern geteilt werden und gering formalisiert sind, eine geringe Reife auf, die mit zunehmender Verbreitung, Formalisierung und Legitimation zunimmt. Diese Dimensionen können auf die verschiedenen wissensbezogenen Ressourcen, wie z.B. Kompetenzen, Produkte, Patente oder Best Practices, angewandt werden (siehe für Beispiele Abb. 6) und werden im weiteren Verlauf der Arbeit aufgegriffen, wenn es darum geht, Risiken, die diese Ressourcen betreffen, zu steuern. Dabei bestehen je nach Ausprägung dieser Dimensionen unterschiedliche Herausforderungen, die im Rahmen von Kapitel 5 thematisiert werden.

2.2.5 Besonderheiten wissensbezogener Ressourcen

Wissensbezogene Ressourcen weisen gegenüber immateriellen und materiellen Ressourcen einige Besonderheiten auf, die es zu berücksichtigen gilt, wenn im Falle des WM eine gezielte Bewirtschaftung oder im Falle der Steuerung von Wissensrisiken spezifische Schutzmaßnahmen ergriffen werden sollen. Dieser Abschnitt hat daher zum Ziel, allgemeine Unterschiede zwischen materiellen und immateriellen Ressourcen zu erörtern und spezifische Besonderheiten wissensbezogener Ressourcen zu fokussieren.

- **Abnutzung**: Materielle Ressourcen, wie z.B. Produktionsanlagen oder Gebäude, unterliegen einer natürlichen altersbedingten Abnutzung, während dies auf immaterielle Ressourcen nicht analog übertragbar bzw. sogar gegenteilig ist (Teece 2002, 15f). Insbesondere bei Kompetenzen als wissensbezogenen Ressourcen, liegt eine inverse Beziehung vor, da sie durch Gebrauch erweitert werden und auch ihr Wert zunehmen kann, während dieser bei Nichtnutzung abnehmen kann (Bamberger, Wrona 1996, 387; Mentzas et al. 2003, 21). Andererseits können immaterielle Ressourcen auch vergleichsweise schneller als materielle Ressourcen entwertet werden (Lev 2004a, 7). Dies wird insbesondere bei technischen Innovationen deutlich, die alte Technologien obsolet werden lassen oder auch beim Wertverlust einer Marke im Falle von Skandalen.
- **öffentliche Nutzbarkeit**: Des Weiteren kann immateriellen Ressourcen allgemein zum Teil die Eigenschaften eines öffentlichen Gutes zugeschrieben werden, was bedeutet, dass die Nutzung einer Partei nicht gleichzeitig die Nutzbarkeit für eine andere Partei reduziert, wie dies bei materiellen Ressourcen der Fall ist. Letztere sind ferner rivalisierend und knapp, während dies auf immaterielle Ressourcen nicht zutrifft, da diese zur selben Zeit mehrfach genutzt werden können und sind somit im Vergleich zu materiellen Ressourcen flexibler einsetzbar sind (Bamberger, Wrona 1996, 687; Lev 2001, 22ff). Bezieht man diese Eigenschaft speziell auf Wissen, so ist der Aspekt der Entwertung besonders zu beachten. So kann durch die öffentliche Nutzbarkeit oder die Zugänglichkeit von sensitivem Wissen dessen Wert reduziert werden (Teece 2002, 15).
- **Dynamik**: Im Vergleich zu traditionellen Ressourcen sind wissensbezogene Ressourcen nicht als statisch, sondern als dynamisch anzusehen, da sie interagieren, sich laufend verändern und transformiert werden (von Krogh, Roos 1996, 34; Marr et al. 2004, 563)[26]. Dabei ist die Dynamik insbesondere darauf zurückzuführen, dass Wissen durch soziale Interaktionen zwischen Individuen und Organisationen generiert wird und kontextspezifisch ist, also von einer bestimmten Zeit und einem bestimmten Ort abhängt (Nonaka et al. 2000, 7).
- **Transferierbarkeit**: Weitere Unterschiede ergeben sich in Bezug auf die Transferierbarkeit und die Transferkosten. Wissensbezogene Ressourcen weisen immer einen gewissen impliziten Gehalt

[26] Auch Hall hat diesen Gedanken bei der Betrachtung immaterieller Ressourcen aufgenommen und unterscheidet zwischen statischem objektbezogenem und dynamischem personen- bzw. prozessbezogenem Wissen (Hall 1993, 609).

auf und sind in einen Kontext eingebettet, weshalb sie einer Interpretation bedürfen (Polanyi 1966, 24f). Je stärker diese Eigenschaften ausgeprägt sind, desto schwerer ist ein erfolgreicher bzw. vollständiger Transfer zu erreichen. Während die Transferkosten von materiellen Ressourcen relativ einfach bestimmt werden können, werden diese Kosten bei wissensbezogenen Ressourcen vom impliziten Gehalt, der Komplexität, der Kontextabhängigkeit sowie der Aufnahmekapazität[27] des Empfängers beeinflusst und sind somit vergleichsweise schwer kalkulierbar (Rehäuser, Krcmar 1996, 11; Grant 1997, 451; Teece 2002, 15f). Dadurch bedingt, dass beim Wissenstransfer komplexe Lernprozesse eine Rolle spielen, ist der erforderliche Zeitbedarf im Vergleich zu traditionellen Ressourcen oftmals vielfach höher.

- **Eigentums- / Schutzrechte**: Ein weiterer Unterschied zwischen diesen Ressourcentypen ist bei den Eigentumsrechten und deren Durchsetzung festzustellen. Diese sind in Bezug auf die materiellen Ressourcen umfassend und vergleichsweise leicht durchsetzbar[28], während die Eigentums- bzw. Schutzrechte für immaterielle Ressourcen (z.B. Patente, Copyrights) nur zum Teil einen Ausschluss Dritter ermöglichen und lückenhaft sind (Teece 2002, 16; Lev 2005, 301). Diese erschwerte Durchsetzbarkeit ist vorwiegend darauf zurückzuführen, dass Wissen selbst organisierend durch Sprache übertragbar und somit nur schwer fassbar ist (Alstete 2003, 2). Die Problematik verstärkt sich zusätzlich, wenn Schutzrechte international definiert und durchgesetzt werden sollen (Baughn et al. 1997, 104).
- **Handelbarkeit**: Ein weiterer Aspekt zur Abgrenzung ist in der eingeschränkten Handelbarkeit von immateriellen Ressourcen zu sehen. Während materielle Ressourcen auf Märkten gekauft bzw. verkauft werden können, ist dies bei immateriellen Ressourcen nur schwer möglich, da sie oftmals in einen spezifischen Kontext eingebettet sind, vollständige Verträge mit zusicherbaren erwarteten Erträgen nicht möglich sind, Schutzrechte in geringerem Umfang greifen und zudem die Informationsasymmetrien bezüglich deren Eigenschaften ausgeprägter sind (Nonaka et al. 2000, 16f; Teece 2000b, 132; Lev 2001, 43f; 2005, 301). Zudem wird die Handelbarkeit immaterieller Ressourcen durch deren Unternehmensspezifität oder eine sehr umfassende Kontexteinbettung und eine damit zusammenhängende erschwerte Herauslösbarkeit aus dem Kontext begrenzt (Dierickx, Cool 1989, 1505; Knaese 1996, 19).
- **Vervielfältigungskosten**: Weiterhin sind immaterielle bzw. wissensbezogene Ressourcen zum Teil auch dadurch gekennzeichnet, dass ihre Generierung mit einem hohem Aufwand (First Copy Cost) also mit hohen Fixkosten verbunden ist, wobei die Verbreitung zu geringen variablen Kosten erfolgen kann (Grant 1997, 451; Shapiro, Varian 1999, 20f; Mentzas et al. 2003, 21; Müller 2006, 9). Dies wird am Beispiel der Erarbeitung einer Studie deutlich, deren Erstellung einen ho-

[27] Cohen und Levinthal (1990) erörtern in diesem Kontext das Konzept der Absorptive Capacity.
[28] z.B. Grundbucheinträge bei Grundstücken, Kaufverträge bei Maschinen.

hen Aufwand (Interviews, Auswertung, Aufarbeitung etc.) nach sich zieht, während deren Verbreitung (v.a. auf elektronischem Weg) vergleichsweise geringe bzw. vernachlässigbare zusätzliche Kosten verursacht.

- **Wertbestimmung**: Ebenso wie bei materiellen Ressourcen ist neben dem bloßen Vorhandensein der immateriellen Ressource auch eine gewisse strategische Relevanz erforderlich, um einen Beitrag zu den Wettbewerbsvorteilen zu leisten und somit als wertvoll charakterisiert zu werden (Hümmer 2001, 57). Die eigentliche Wertgenerierung erfolgt bei immateriellen Ressourcen durch die Interaktion und Kombination, die ebenso organisatorische Fähigkeiten erfordert (DeNisi et al. 2003, 9; Kaplan, Norton 2004, 54). Zudem sind immaterielle Ressourcen oftmals in materiellen inkorporiert, wodurch die Abgrenzung erschwert wird. In der bilanziellen Praxis erfolgt dabei die Abgrenzung in Abhängigkeit der Bedeutung der immateriellen Komponente (Arbeitskreis 2001, 990)[29]. Des Weiteren ist eine Wertbeimessung bei immateriellen Ressourcen aufgrund unvollkommener Informationen schwer möglich und wird insbesondere durch die sich aus dem kombinierten Einsatz der Ressourcen ergebende Komplexität erschwert (Bamberger, Wrona 1996, 387). Weiterhin wird die Bewertung dadurch erschwert, dass sich immaterielle Ressourcen nicht direkt auf das finanzielle Ergebnis auswirken, sondern ihrerseits von Kontextfaktoren abhängig sind. So wird beispielsweise der Wert von Kompetenzen durch organisatorische Rahmenbedingungen oder auch die Unternehmensstrategie beeinflusst (Möller 2004, 486). Speziell bei wissensbezogenen Ressourcen wird die Wertbestimmung dadurch erschwert, dass Wissen kontextabhängig ist, laufend verändert werden muss und durch seine Nutzung nicht verbraucht, sondern wertvoller wird. Der Wert variiert darüber hinaus über Unternehmen und Branchen hinweg und wird von der jeweiligen Situation beeinflusst (Sanchez 1995, 5f; Zahn et al. 2000, 257; Choi et al. 2005, 71; Müller-Stingl, Neumann 2006, 55).

Unter diesen Besonderheiten ist aus ökonomischer Perspektive insbesondere die erschwerte Wertbeimessung als relevant anzusehen, da sie ein Defizit darstellt, das sich auf die gezielte Bewirtschaftung von wissensbezogenen Ressourcen bzw. auf die Steuerung von Risiken, die diese Ressourcen betreffen, auswirkt. Zur Überwindung dieses Defizits wurden bereits verschiedene Ansätze entwickelt, die gesondert in Abschnitt 2.3 betrachtet werden.

In den vorangegangenen Abschnitten wurde ausgehend vom ressourcenbasierten Ansatz die Bedeutung von wissensbezogenen Ressourcen deren Eigenschaften, Dimensionen und Besonderheiten hervorgehoben, wobei sich die Bedeutung in zweierlei Hinsicht zeigt. Zum einen wird sie im Rahmen des strategischen Managements durch den wissensbasierten Ansatz gewürdigt. Zum anderen wird deren Bedeutung sowohl in Theorie als auch Praxis durch die Implementierung verschiedener Initiativen zur gezielten Bewirtschaftung der Ressource Wissen deutlich. Eine derartige Bewirtschaftung ist dabei

[29] Siehe hierzu auch (IAS 38.4) und Abschnitt 2.3.3.

insbesondere für Unternehmen relevant, für die Wissen einen hohen Stellenwert in Bezug auf die Generierung der Wertschöpfung bzw. den Aufbau oder Erhalt der Wettbewerbsvorteile einnimmt. Diese Unternehmen werden vielfach auch als wissensintensive Unternehmen bezeichnet. Im nachfolgenden Abschnitt werden Charakteristika erörtert, die die Wissensintensität von Unternehmen beeinflussen.

2.2.6 Wissensintensität von Unternehmen

In einigen Unternehmen wird Wissen als die bedeutendste bzw. konstituierende Ressource angesehen, die die Basis für Wettbewerbsvorteile bildet (Grant 1996b, 375; von Krogh, Roos 1996, 32; Stewart 1998; Marsh, Ranft 1999, 43; Robertson, Hammersley 2000, 241; Zahn et al. 2000, 384). Diese Unternehmen werden vielfach als wissensintensiv bezeichnet (siehe z.B. Starbuck 1992, 715ff)[30]. Der Begriff Wissensintensität wird einerseits in der Literatur sehr heterogen diskutiert, andererseits zum Teil knapp bzw. unreflektiert abgehandelt. Dabei fällt es generell schwer, zu definieren, wann ein Unternehmen als wissensintensiv eingestuft wird, weil jede Schätzung von Intensität anfechtbar ist (Alvesson 2001, 864). Aus einer ökonomischen Perspektive wird von einem wissensintensiven Unternehmen erwartet, dass es Wissen für die zukünftige Kommerzialisierung nutzt und aktuelle Gewinne aus dem bestehenden Wissen generiert (Sullivan 1999, 134). Die heterogene Begriffsauffassung wird weiterhin darin deutlich, dass einige Autoren spezifische Branchen oder Unternehmenstypen, wie z.B. High Tech-, Beratungs- oder Softwareunternehmen, als wissensintensiv bezeichnen, während andere beispielsweise auf die Anzahl akademischer Abschlüsse in Unternehmen oder Anzahl der Patente, also auf Abgrenzungskriterien, abstellen (Bonora, Revang 1993, 191f; Zahn et al. 2000, 243; Mertins, Alwert 2003, 578)[31]. Zack (2003, 67ff) widerspricht der Fokussierung auf bestimmte Branchen und vertritt die Ansicht, dass Unternehmen ungeachtet der Branchenzugehörigkeit wissensintensiv sein können oder nicht. Vielmehr nähert er sich ebenso wie Swart und Kinnie über verschiedene Kriterien an, die erfüllt sein müssen, um von einem wissensintensiven Unternehmen zu sprechen (Swart, Kinnie 2003, 62). Auf der Basis dieser Auffassungen werden nachfolgend auf Basis der Literatur identifizierte Kriterien herangezogen, die losgelöst von Branchen eine Einschätzung der Wissensintensität von Unternehmen und Organisationen ermöglichen sollen.

- **Anteil hoch qualifizierter Mitarbeiter**: Unternehmen, deren Erfolg und Zukunftspotential auf den Kenntnissen und Fähigkeiten ihrer hoch qualifizierten Mitarbeiter (Wissensarbeiter) basiert, sind vergleichsweise wissensintensiver (Sveiby 1997, 19; Scholz, Bechtel 2002, 11; Swart, Kinnie

[30] In der deutschsprachigen und angloamerikanischen Literatur bestehen eine Vielzahl weiterer Begriffe, wie z.B. wissensbewusst, -orientiert, -verarbeitend, Wissensunternehmen, wissensbasierte Unternehmen etc., wobei die Begriffe im Wesentlichen auf Wissensintensität hindeuten. Für weitere Details siehe (Civi 2000, 167f; Rylander, Peppard 2005; Davenport, Holsapple 2006, 451).

[31] Eine Studie von Capgemini kommt zu dem Ergebnis, dass insbesondere in High Tech Unternehmen immaterielle Ressourcen eine hohe Bedeutung aufweisen, während zwischen Dienstleistungs- und Industrieunternehmen kein signifikanter Unterschied festgestellt werden kann (Capgemini 2005, 13).

2003, 62). Der Anteil hoch qualifizierter Mitarbeiter ergibt sich aus dem Verhältnis der entsprechenden Ausbildungsabschlüsse (z.B. Schulbildung, akademischer Grad etc.).

- **Anteil an Experten**: Die Wissensintensität nimmt zudem mit dem Anteil an Experten zu, die über Wert generierende Kompetenzen verfügen und im Unternehmen beschäftigt sind. Starbuck fokussiert demnach anstelle der formalen Qualifikation der Mitarbeiter auf den Grad an Expertise. Dabei ist es allerdings entscheidend, wie weit der Begriff Expertise definiert wird, da bei einer sehr umfassenden Definition dieses Kriterium auf eine Vielzahl an Unternehmen zutrifft und dementsprechend keine Differenzierungskriterium mehr darstellt (Starbuck 1992, 718ff).
- **Anteil Wissensarbeit**: Die Wissensintensität wird nicht nur durch die Anzahl hoch qualifizierter Mitarbeiter oder Experten bestimmt, sondern vielmehr durch die Tätigkeiten, denen diese Mitarbeiter nachgehen. Nach dem Verständnis von Sveiby bedeutet dies, dass die Mitarbeiter unter Einsatz ihrer Kompetenzen Informationen in Wissen umzuwandeln (Sveiby 1997, 19).
- **etablierte Wissensprozesse:** Wissensintensive Unternehmen zeichnen sich dadurch aus, dass die Anwendung bestehenden Wissens und die Generierung neuen Wissens zugrunde liegende Prozesse darstellen und diese zur Erstellung der Wertschöpfung beitragen (Swart, Kinnie 2003, 62; Zack 2003, 69). Ziel ist es, durch diese Prozesse die Anwendung von Wissen einerseits und die interne Verbreitung im Unternehmen andererseits zu fördern (Zack 2003, 69).
- **Austausch mit Partnern**: Die Wissensintensität von Unternehmen erhöht sich weiterhin dadurch, dass diese nicht isoliert agieren, sondern mit Partnern, Kunden und Lieferanten in Austausch stehen (Sveiby 1997, 19; Swart, Kinnie 2003, 60, 63). Somit macht der Wissenstransfer nicht an den Grenzen des Unternehmens halt, sondern bezieht auch externe Partner mit ein (Zack 2003, 69). Dies ist v.a. auch darauf zurückzuführen, dass es in wissensintensiven Unternehmen oftmals aus Zeit- und Aufwandsgründen nicht möglich ist, das erforderliche Wissen intern zu entwickeln (Badaracco 1991, 123; Grant, Baden-Fuller 1995, 17ff).
- **wissensorientierte Strategie**: Im Hinblick auf die strategische Ausrichtung sind wissensintensive Unternehmen dadurch gekennzeichnet, dass sie die WM-Prozesse bzw. die -strategie und Unternehmensstrategie miteinander verknüpfen. In diesen Unternehmen wird Wissen als Schlüsselressource angesehen und stellt auch deswegen einen Hauptbestandteil ihrer Strategie dar (Zack 2003, 69). Demzufolge betrachten diese Unternehmen ihr tägliches Geschäft aus einer wissensorientierten Perspektive und sehen es als potentielle Lerngelegenheit an. Wissen und Lernen stellen das Hauptkriterium für die Bewertung der Organisation, Personalakquise, Geschäftsausrichtung, Bezug zum Kunden etc. dar (Zack 2003, 69).
- **wissensbasierte Produkte**: Unternehmen können dann als vergleichsweise wissensintensiver angesehen werden, wenn die materiellen oder immateriellen Produkte, die erstellt werden, zu einem erheblichen Teil auf der Anwendung von Wissen basieren. So kann im Falle von produzierenden

Unternehmen ein hoher Forschungs- und Entwicklungsaufwand ein Indiz für die Wissensintensität sein (Alvesson 2004, 17). Auch die Erstellung von maßgeschneiderten Produkten (z.B. spezifische Kundenlösungen von Beratungs- oder Softwareunternehmen) ist als ein Anhaltspunkt zu sehen (Swart, Kinnie 2003, 62).

- **Anzahl an Patente**: Neben Produkten ist auch die Anzahl an Patenten, über die das Unternehmen verfügt, ein Indikator für dessen Wissensintensität, der als Vergleichsmaßstab zu anderen Unternehmen der Branche herangezogen werden kann. Eine vergleichsweise hohe Anzahl an Patenten, lässt auf eine hohe Innovationsfähigkeit und demzufolge Wissensintensität schließen[32].

Die Vergleichbarkeit von Unternehmen bzgl. deren Wissensintensität ist allerdings nur schwer möglich, da es sich nur um Näherungskriterien handelt und diese zudem auch in unterschiedlicher Intensität zutreffen, wobei eine Gewichtung zwischen den Kriterien fehlt und somit empirisch zu validieren wäre. So kann die Vergleichbarkeit dadurch erschwert werden, dass Unternehmen in Bezug auf einzelne Kriterien als überdurchschnittlich einzustufen sind, während andere Kriterien nicht zutreffen. Dies bedeutet z.B., dass ein Unternehmen nur wenige Austauschbeziehungen unterhält und über wenige hoch qualifizierte Mitarbeiter verfügt, aber dennoch eine hohe Wissensintensität aufweisen kann, weil es über eine Vielzahl an Patenten verfügt, deren zugrunde liegendes Wissen von wenigen Experten entwickelt wird. Auch Unterschiede in Bezug auf die Wissensträger erschweren in diesem Zusammenhang die Vergleichbarkeit (Bonora, Revang 1993, 192). So kann ein Unternehmen zwar über wenige hoch qualifizierte Mitarbeiter, jedoch über dokumentiertes Wissen in großem Umfang verfügen. Nichtsdestotrotz erscheint die Anwendung von Näherungskriterien bei der Einschätzung der Wissensintensität zielführender als eine pauschalisierte Betrachtung einzelner Branchen. Entsprechend dieser Einteilung ist die systematische Auseinandersetzung mit Wissensrisiken für diejenigen Unternehmen von besonderer Relevanz, auf die diese komplementären Kriterien besonders zutreffen.

2.3 Bewertung immaterieller und wissensbezogener Ressourcen

Es kann eine Vielzahl von Fällen herangezogen werden, die eine Bewertung immaterieller Ressourcen erforderlich machen. Beispiele sind Fusionen, Akquisitionen, Börsengänge, Kauf oder Lizenzierung immaterieller Ressourcen, wie z.B. Marken, Patente oder Copyrights (Contractor 2000, 243; Bruns et al. 2003, 137; Persch 2003, 324). Dabei stellt der Wandel zur Hochtechnologie- und Wissensgesellschaft eine Herausforderung dar, da aufgrund des gestiegenen Wertschöpfungsbeitrags von Wissen traditionelle Bewertungsverfahren, die auf materielle Ressourcen ausgerichtet sind, nicht geeignet sind, den tatsächlichen Wert des Unternehmens widerzuspiegeln (Küting, Dürr 2003, 1ff; Roos et al. 2004, 129). Die Folge ist, dass es oftmals zu Über- bzw. Unterbewertungen kommt. Eine Überbewer-

[32] So hat in 2006 IBM 3.621 Patente angemeldet und war damit weltweit Spitzenreiter. Siehe hierzu http://www.golem.de/0701/.49922.html.

tung ist in der Vergangenheit insbesondere bei so genannten „dot-com Unternehmen“ erfolgt, während immaterielle Ressourcen bei Unternehmen aus etablierten Wirtschaftssektoren zum Teil unterbewertet werden (Lev 2004b, 109f).

Der Marktwert vieler Unternehmen liegt weit über dem Buchwert, was darauf zurückgeführt werden kann, dass diese Unternehmen über immaterielle Ressourcen verfügen und diese zur Generierung der Wertschöpfung einsetzen (Lev 2004b, 110). Bereits Ende der 90’ er Jahre ergaben Schätzungen, dass ¾ des Marktwertes der Fortune 100 Unternehmen auf immaterielle Ressourcen wie Patente, Copyrights etc. zurückgeführt werden können (Reitzig 2004, 35). Dabei zeigt sich der Trend, dass die Marktwerte von Unternehmen, die immaterielle Produkte erstellen bzw. Dienstleistungen erbringen, vergleichsweise stärker vom Buchwert abweichen. So betrug 1999 der Marktwert von Coca-Cola, Microsoft oder SAP das 15-21-fache des Buchwerts, während sich beim Automobilhersteller Ford das Verhältnis auf 1:3 belief (Contractor 2000, 243; Wucknitz 2002, 4; Esser, Hackenberger 2004, 402)[33]. Die Bestrebungen immaterielle Ressourcen des Unternehmens zu messen und auf dieser Basis gezielt Managementmaßnahmen zu ergreifen, finden ihre Ursprünge in Arbeiten zum Humankapital z.B. Schultz (1961) oder Flamholtz (1974). Itami[34] rückte alle immateriellen Ressourcen (invisible assets) in den Mittelpunkt und sensibilisierte für deren Bedeutung im Kontext japanischer Unternehmen. Auch Hall (1989) diskutierte immaterielle Ressourcen als zentrale Werttreiber des Unternehmens. Unter den verschiedenen Ansätzen, die auf eine Bewertung immaterieller Ressourcen im Allgemeinen und wissensbezogener Ressourcen im Speziellen abzielen, hat insbesondere der Ansatz zum intellektuellen Kapital weite Verbreitung gefunden (siehe 2.3.1). Dieser Absatz stellt die Ausgangsbasis für weitere spezifische Bewertungsansätze dar, die von Unternehmen auf freiwilliger Basis eingesetzt werden und in Abschnitt 2.3.2 betrachtet werden. Im Kontext verschiedener Bilanzierungsrichtlinien können immaterielle Werte aktiviert werden und tragen somit zur Erhöhung des Buchwertes bei (siehe 2.3.3). Während bei Rechnungslegungsstandards die Aktivierungsfähigkeit immaterieller Vermögenswerte vordergründig ist, zielt die freiwillige Berichterstattung, die auch die Wissensbilanz einschließt, auf eine unternehmensinterne und -externe Kommunikation dieser Werte ab, um so Informationsasymmetrien zu schließen (siehe 2.3.4). Abschließend werden die verschiedenen Bewertungsansätze in Bezug auf wissensbezogene Ressourcen integriert betrachtet (siehe 2.3.5).

2.3.1 Ansatz des intellektuellen Kapitals

Der Begriff intellektuelles Kapital wurde erstmals durch Galbraith (1969) aufgegriffen und durch vorwiegend aus dem skandinavischen Raum stammende Vertreter populär gemacht. Dabei setzten

[33] In 2006 betrug die Marktkapitalisierung bei SAP 51 Mrd. €, während das bilanzielle Eigenkapital 6,1 Mrd. € betrug. Somit ergibt sich ein Verhältnis von 8,36 (SAP 2007, 105).

[34] Itamis erstes Werk erschien 1980 in Japan und 1987 im englischsprachigen Raum (Itami 1987).

sich Sveiby und Lloyd 1986[35] mit dem intellektuellen Kapital auseinander und betonten, dass der Wert des Unternehmens primär von den Fähigkeiten der Mitarbeiter abhängig sei (Sveiby, Lloyd 1990). 1987 erfolgte die Gründung der Konrad Group in Schweden, die sich mit der Bewertung immateriellen Ressourcen befasste und das „The invisible balance sheet" (1989)[36] veröffentlichte, das der mangelnden Berücksichtigung immaterieller Werte in Bilanzen Rechnung trägt (Kreft 2004, 24; Müller 2006, 12). 1991 wurde Edvinsson Vice President bei Skandia[37] und trieb die Berücksichtigung immaterieller Ressourcen voran, was zur Folge hatte, dass zusätzlich zur Bilanz Reports zum intellektuellen Kapital entwickelt wurden (Edvinsson, Freij 1999, 1994; Abell, Oxbow 2002, 28; Müller 2006, 12). Der Marktwert eines Unternehmens wird neben dem Finanzkapital primär durch das intellektuelle Kapital determiniert. Dieses Verständnis spiegelt sich auch in vielen konzeptionellen Modellen zur Strukturierung der Komponenten des intellektuellen Kapitals wider (siehe Abb. 7). Auf einer ersten Verfeinerungsstufe wird intellektuelles Kapital in die Hauptkomponenten Human- und Strukturkapital unterteilt (Edvinsson 1997; Stewart 1997).

Unter Humankapital sind die kurzfristig einsetzbaren, fachlichen und sozialen Potentiale der Mitarbeiter und Führungskräfte eines Unternehmens zu verstehen (Barthel et al. 2004, 21). Dabei ist zu beachten, dass Kompetenzen nicht im Eigentum des Unternehmens stehen, sondern vielmehr durch eine Kompensation über Löhne und Gehälter für eine bestimmte Zeit „gemietet" sind bzw. die Verfügungsrechte über Verträge durchgesetzt werden (Edvinsson 1997, 369; Sveiby 1997, 10; Joia 2000, 71; Persch 2003, 325). Im Hinblick auf einen nachhaltigen Erfolg, kommt der Stabilität des Humankapitals eine Bedeutung zu. Indikatoren zur Messung der Stabilität sind z.B. Betriebszugehörigkeit, Durchschnittsalter, Fluktuationsrate, Absentismusrate oder Mitarbeiterzufriedenheit (Walde 2004, 153f). Strukturkapital stellt z.B. in Form von Abläufen oder Patenten verankertes Wissen dar und ist auch noch dann vorhanden, wenn die Mitarbeiter das Unternehmen verlassen haben (Edvinsson, Malone 1997, 11; Wiig 1997, 401). Es ist einerseits das Ergebnis des Einsatzes des Humankapitals, stellt aber andererseits wiederum die Infrastruktur dar, mittels derer die Produktivität des Humankapitals erhöht werden kann (Edvinsson, Brünig 2000, 28). Das Strukturkapital wird in Beziehungs- und Organisationskapital untergliedert. Einige Autoren, wie z.B. (Wiig 1997), führen Kundenkapital als eigene Kategorie an, wobei eine Begrenzung auf Kunden nicht zweckmäßig erscheint, da auch Beziehungen zu Lieferanten und Partnern immaterielle Werte darstellen können[38] (Sveiby 1997, 11; Piber 2004, 501; Roos et al. 2004, 130). Beziehungskapital stellt denjenigen Wert dar, der durch die Beziehungen des Unternehmens generiert wird. Organisationskapital kann in Innovations- und Prozesskapital unterteilt werden, wobei ersteres Ressourcen wie Patente, Lizenzen oder auch Marken

[35] Im Original erschienen: Sveiby, K.-E., Risling, A.: Kunskapsföretaget, Malmö 1986.
[36] Im Original erschienen: Konrad Group: Den osynliga balansräkningen, Malmö, 1988.
[37] Neben dem schwedischen Versicherungsunternehmen Skandia zählt auch die Canadian Bank of Commerce zu den Pionierunternehmen im Bereich intellektuelles Kapital (Barthel et al. 2004, 30).
[38] Zum Teil wird Partner- bzw. Allianzkapital neben das Kundenkapital gestellt z.B. (Stoi 2003).

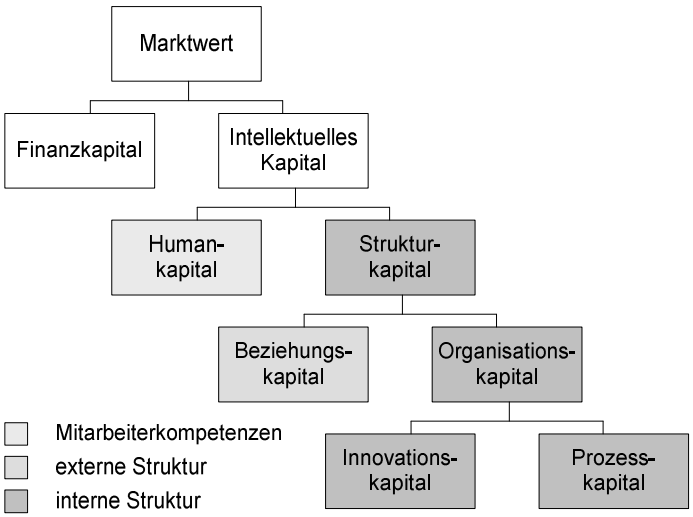


Abb. 7 Aufteilung des intellektuellen Kapitals[39]

umfasst. Prozesskapital basiert auf den wertschöpfenden Prozessen des Unternehmens, wie z.B. Organisationsstruktur, Managementpraktiken, Systemen, IT-Infrastruktur und Prozeduren (Wiig 1997, 401).

Im Hinblick auf das intellektuelle Kapital kann nach Sveiby (1997, 10f) eine Dreiteilung in Mitarbeiterkompetenzen, interne und externe Struktur vorgenommen werden (siehe auch Abb. 7). Unter der internen Struktur werden alle immateriellen Ressourcen subsumiert, die im Eigentum des Unternehmens stehen. Somit wird das Strukturkapital mit Ausnahme des Kundenkapitals dieser Kategorie zugeordnet (Sveiby 1997, 10). Immaterielle Ressourcen der externen Struktur stehen nicht im Eigentum des Unternehmens und umfassen das Beziehungskapital zu Kunden, Lieferanten und Partnern. Zudem werden extern gesteuerte immaterielle Werte wie Marken und Reputation unter dieser Kategorie subsumiert (Sveiby 1997, 11). Mitarbeiterkompetenzen stellen die dritte Kategorie immaterieller Werte dar, wobei das Humankapital eine Sonderstellung unter den immateriellen Ressourcen einnimmt, da neben der begrenzten Verfügungsmöglichkeit auch die Verfügungsdauer bedingt durch potentielle Kündigungen unsicher ist (Huber 1998, 64). Trotz dieser Unsicherheitsfaktoren kommt den Mitarbeiterkompetenzen eine sehr hohe Bedeutung in Bezug auf das Management immaterieller Ressourcen zu, da ohne diese Unternehmen nicht am Markt agieren könnten (Sveiby 1997, 10). Die allgemeine Struktur des intellektuellen Kapitals und die Dreiteilung nach Sveiby sind in Abb. 7 zusammengefasst. Basierend auf diesem Grundverständnis wurden gegen Ende der 90'er Jahre erste Bewertungsansätze entwickelt, die Gegenstand des folgenden Abschnittes sind.

2.3.2 Bewertungsansätze

Mit der Bewertung immaterieller Ressourcen werden sowohl interne als auch externe Ziele verfolgt. Dabei stellen das Verstehen der Wirkung immaterieller Ressourcen, die Erkennung von Werttreibern und darauf basierende Performanceverbesserungen bzw. Strategieausrichtungen interne Ziele dar, während die Bereitstellung von Informationen über den Stand der Entwicklung nicht aktivierbarer Werte für externe Stakeholder bzw. die Kommunikation des „realen" Wertes des Unternehmen externe Ziele darstellen können (Arbeitskreis 2003, 1233f; Andriessen 2004, 232ff; Marr et al. 2004, 553;

[39] In Anlehnung an (Edvinsson, Malone 1997, 73; Sveiby 1997, 10f; Wiig 1997, 404).

Alwert et al. 2005, 9ff; Bukh et al. 2005, 57f; Hunter et al. 2005, 12). So kann beispielsweise diese zusätzliche Berichterstattung über nicht ansetzbare immaterielle Werte Unternehmen eine verbesserte Fremdkapitalaufnahme ermöglichen (Reinhardt 2002, 33; Kaufmann, Schneider 2006, 24)[40]. Sullivan betont neben der Außenwirksamkeit eine defensive und eine offensive Nutzung des intellektuellen Kapitals. Erstere fokussiert auf die Sicherung einer exklusiven Nutzung bestimmter Ressourcen (z.B. durch Patentierung), während die offensive Nutzung z.B. die Kapitalisierung durch Lizenzierung von Technologien in andere Märkte einschließt (Sullivan 1999, 137).

Die Bedeutung immaterieller Ressourcen ist mittlerweile weit anerkannt, was sich in einer Studie von Capgemini zeigt, nach der 69% der befragten Unternehmen die Bedeutung immaterieller Ressourcen für den Unternehmenserfolg höher als den materieller einschätzten (Capgemini 2005, 11f)[41]. Dabei kann auf Basis dieser Studie keine allgemein gültige Aussage getroffen, in welchen Branchen die Bedeutung besonders hoch ist[42]. Nach einer Studie von PWC (2003, 16) werden immaterielle Ressourcen wie Humankapital, direkt wertschöpfende Prozesse oder Innovationskapital für den Unternehmenserfolg bedeutender als finanzielle oder materielle Ressourcen eingeschätzt[43].

Im Hinblick auf die Bewertung immaterieller Ressourcen unterscheiden North et al. (1998, 159f) zwischen deduktiv summarischen Verfahren, deren Bewertungsbasis die Differenz zwischen Markt- und Buchwert bildet und induktiv analytischen Ansätzen, mittels derer immaterielle Ressourcen meist über nicht-finanzielle Indikatoren mit dem Ziel, Anhaltspunkte zur Steuerung zu gewinnen, bewertet werden. Mertins und Alwert (2003, 579) unterscheiden zwischen Strukturansätzen, Methoden zur monetären Gesamtbewertung und Steuerungsansätzen. Erstere stellen auf die Kategorisierung immaterieller Ressourcen und die Beschreibung der einzelnen Komponenten mittels quantitativer und qualitativer Indikatoren ab (Alwert 2005, 23). Monetäre Bewertungsansätze entstammen vorwiegend dem angloamerikanischen Raum und versuchen auf der Basis von Kosten, Marktwerten oder zukünftigen Erträgen, den Wert der immateriellen Ressourcen zu bestimmen (Alwert 2005, 24). Steuerungsansätze wie die Balance Scorecard zielen auf die Steuerung von Organisationen unter Einbezug immaterieller Einflussgrößen ab (Mertins, Alwert 2003, 579). Die am weitesten verbreitete Unterteilung geht auf Sveiby (2007)[44] zurück und ist im Vergleich zur ähnlichen Kategorisierung von Mertins und Alwert detaillierter. Demnach kann unterschieden werden in:

a) Marktkapitalisierungsmethoden (MCM), die den Wert des intellektuellen Kapitals auf Basis der Marktkapitalisierung[45] und dem Unterschied zum Anteilskapital der Aktionäre errechnen,

[40] Siehe hierzu auch 2.3.4.
[41] Nach Nemetz (2006, 13) entfallen mehr als 2/3 des Bruttoinlandsprodukts der USA auf immaterielle Ressourcen.
[42] Siehe hierzu auch die Diskussion zur Wissensintensität von Unternehmen in Abschnitt 2.2.6.
[43] Auch die Studie von Capgemini kommt zu diesem Ergebnis, wobei Kundenzufriedenheit, Mitarbeiter Know-how und Top Management Kompetenz als bedeutendste Faktoren identifiziert wurden (Capgemini 2005, 21).
[44] Sveiby setzt auf den Klassifikationen von Luthy (1998) und Williams (2000) auf.
[45] Marktkapitalisierung entspricht dem Produkt des Aktienkurses und der Anzahl der ausgegebenen Aktien.

b) direkte Methoden (DIC), die eine monetäre Bewertung einzelner Komponenten zum Gegenstand haben,
c) ROA[46]-Methoden (ROA), die den Wert anhand der Kennzahl ROA ermitteln und diese Werte mit anderen Unternehmen vergleichen sowie
d) Scorecard-Methoden (SC), die mittels Verwendung verschiedener Indikatoren vorwiegend zur qualitativen Berichterstattung herangezogen werden.

In den nachfolgenden Abschnitten (2.3.2.2-2.3.2.4) werden ausgewählte Ansätze entsprechend dieser Klassifikation in Abhängigkeit ihrer Verbreitung in der Literatur dargestellt[47].

2.3.2.1 Marktkapitalisierungsmethoden

Marktkapitalisierungsmethoden (MCM) errechnen den Wert des intellektuellen Kapitals auf der Basis des Marktwertes des Unternehmens als Produkt aus aktuellen Aktienkurs und Aktienanzahl. Der Wert des intellektuellen Kapitals ergibt sich somit aus der Differenz aus Markt- und Buchwert (Stewart 1997, 224f). Ähnlichkeiten zum Marktwert-Buchwert-Verhältnis weist auch die Kennzahl Tobins Q auf, die aus dem Quotienten aus dem Marktwert des Unternehmens und Wiederbeschaffungskosten für die Ressourcen gebildet wird. Ist der Quotient größer als 1 wird das Unternehmen höher bewertet als die Summe seiner Vermögensgegenstände. Im umgekehrten Fall ist der Wert des Unternehmens geringer bewertet als die Summe der Wiederbeschaffungskosten (Barthel et al. 2004, 32). Die Berechnung der Differenz der beiden Größen stellt ein alternatives Verfahren zur Ermittlung des Wertes des intellektuellen Kapitals dar (Stewart 1997, 224ff). Das Problem dieser Bewertungsmethoden besteht darin, dass einerseits der als Residualgröße ermittelte Wert des intellektuellen Kapitals sehr hoch aggregiert ist und somit die Aussagekraft und Zuverlässigkeit gering sind. Andererseits ist der Marktwert nicht ausschließlich auf immaterielle Ressourcen zurückzuführen, sondern auch von anderen Faktoren, wie z.B. Konjunktur oder Einschätzungen von Analysten, abhängig, was zur Folge hat, dass der Wert des intellektuellen Kapitals verzerrt ist (Broda 2003, 738). Ferner führen Veränderungen des Zinsniveaus zu Veränderungen des Aktienkurses und stellen somit eine verzerrende Einflussgröße dar. Die breite Anwendung von Bewertungsverfahren dieser Kategorie wird zudem durch die erforderliche Börsennotierung limitiert (Barthel et al. 2004, 32). MCM-Verfahren sind besonders geeignet für Fusionen und Akquisitionen sowie für Vergleiche zwischen Unternehmen. Eine Unterstützung bei der Steuerung der immateriellen Ressourcen bieten diese Methoden allerdings nicht (Möller 2005, 5).

2.3.2.2 direkte Methoden

Direkte Methoden haben zum Ziel, den monetären Wert einzelner Ressourcen oder Ressourcenkategorien des intellektuellen Kapitals zu ermitteln. Durch Aggregation der bewerteten Einzelkomponen-

[46] ROA steht für Return on assets.
[47] Für eine Übersicht zu den verschiedenen Bewertungsansätzen siehe (Roos et al. 2004, 140ff; Müller 2006, 20ff).

ten wird in einigen Ansätzen ein Gesamtwert des intellektuellen Kapitals ermittelt. Zur monetären Bewertung werden vielfach indikatorenbasierte Methoden eingesetzt. So wird mittels des „Technology Brokers“ (Brooking 1996) durch die Beantwortung von 20 Fragen zu vier Komponenten des intellektuellen Kapitals dessen Wert ermittelt. Spezialisierte Methoden haben beispielsweise die Ermittlung des Wertes von Patenten zum Gegenstand. So kann nach Bontis (1996) ein „Technologiefaktor“ ermittelt werden, der auf einer Reihe von Indizes beruht, die die Patente beschreiben (z.B. absolute Anzahl, Kosten im Verhältnis zum Umsatz). Hall et al. (2000b) zeigen auf, dass die Zitation von Patenten stärker mit dem Marktwert des Unternehmens korreliert als die reine Anzahl der Patente. Für die Ermittlung des Wertes von Patenten sind drei Bewertungsansätze gängig. Mittels der Kostenmethode werden die Kosten zugrunde gelegt, die für die Entstehung des Patentes (einschließlich der dahinter stehenden Technologie) angefallen sind bzw. für dessen Reproduktion erforderlich wären. Marktpreisverfahren orientieren sich bei der Bewertung an ähnlichen Produkten, die vor kurzem lizenziert oder veräußert wurden, während gewinnorientierte Modelle den zukünftig zu erwartenden Gewinn in die Bewertung einfließen lassen (Koller, Hentschel 2006, 303ff). Methoden aus diesen drei Kategorien werden auch zur Bewertung von Marken herangezogen (Sattler 2005, 48). Dieser Bewertung kommt dadurch bedingt, dass Marken vielfach einen großen Teil des Unternehmenswertes ausmachen, eine erhebliche Bedeutung zu (Barthel et al. 2004, 33f; Sattler 2005, 34).

Direkte Methoden haben zum Vorteil, dass sie im Vergleich zu anderen Verfahren neben bloßen finanziellen Kennzahlen eine umfassendere Abbildung des Zustandes liefern. Nachteilig ist, dass bedingt durch die Kontextabhängigkeit der Indikatoren eine unternehmensspezifische Anpassung erforderlich ist und somit die Vergleichbarkeit erschwert wird (Möller 2005, 5)[48].

2.3.2.3 ROA-Methoden

ROA ist eine Rentabilitätskennzahl zur Unternehmensbewertung, mittels derer ermittelt wird wie effizient das Unternehmen die Aktiva eingesetzt hat, um Gewinne zu realisieren. ROA-Methoden bauen auf einem Vergleich mit dem durchschnittlichen Branchen-ROA auf und sind somit auf unternehmensübergreifende Vergleichswerte angewiesen. Die sich daraus ergebende Differenz wird mit dem durchschnittlichen materiellen Vermögen multipliziert, um den Ertrag aus den immateriellen Ressourcen zu erhalten. Die Division mit den durchschnittlichen Kapitalkosten des Unternehmens ergibt eine Schätzung des Wertes der immateriellen Ressourcen (Möller 2005, 5).

Der Economic Value Added (EVA) als Geschäftsergebnis nach Steuern abzüglich der Kapitalkosten wird im Rahmen dieser Methoden diskutiert, zielt allerdings nicht auf eine direkte Messung des intellektuellen Kapitals ab (Alwert 2005, 28). Im Rahmen von Ansätzen zur Humanvermögensrechnung werden Kennzahlen zur Ermittlung der Rentabilität des eingesetzten Humankapitals ermittelt. Ein

[48] Weitere Details zur Bewertung von Marken siehe auch bei (Göttgens et al. 2001; Wirtz et al. 2001).

Beispiel ist die Kennzahl HCROI[49], mittels derer die Rentabilität des Humankapitals denjenigen Anteil am Gewinn darstellt, der durch Humankapitalkosten verursacht wird. Zu den Humankapitalkosten zählen neben Löhnen und Gehältern auch Fluktuations- und Abwesenheitskosten (Fitz-Enz 2003, 53). Für eine hohe Aussagekraft derartiger Kennzahlen ist es erforderlich, dass Vergleichswerte anderer Unternehmen vorhanden sind. Dies ist insbesondere bei spezialisierten Kennzahlen nur schwer realisierbar und limitiert ebenfalls die Anwendbarkeit der Methoden dieser Kategorie.

2.3.2.4 Scorecard-Methoden

Mittels Scorcard Methoden werden immaterielle Ressourcen identifiziert, Indizes oder Indikatoren, die oftmals aus der Unternehmensstrategie abgeleitet werden, für diese generiert und die Ergebnisse in Scorecards oder Graphen repräsentiert. Im Unterschied zu den direkten Methoden erfolgt keine monetäre Bewertung, sondern vielmehr eine Ausrichtung auf die Steuerung (Roos et al. 2004, 139; Möller 2005, 5). Die verschiedenen Ansätze dieser Kategorie verfolgen zum Teil auch das Ziel, die erhobenen Indikatoren bzw. Indizes als Teil der freiwilligen Berichterstattung (siehe 2.3.3) zur Information der Stakeholder heranzuziehen, die einen Teil des Geschäftsberichts bildet (Abell, Oxbow 2002, 28; Müller 2006, 12).

Einer der bekanntesten Ansätze ist der „Intangible Asset Monitor“ von Sveiby (1997), der auf einer Untergliederung des intellektuellen Kapitals in individuelle Kompetenzen, interne und externe Struktur basiert[50]. Indikatoren aus den Bereichen Wachstum / Entwicklung, Effizienz und Stabilität sind vordefiniert und können vom Unternehmen angepasst werden. Beispiele für Indikatoren sind Mitarbeiterfluktuation, Anzahl Wiederholungskäufe durch Kunden oder Anzahl imagefördernder Kunden. Die Indikatoren sollen dabei Informationen über das zukünftige Entwicklungspotential des Unternehmens geben, das neben der internen Steuerung auch gezielt an Stakeholder kommuniziert werden kann. Eine ähnliche Methode stellt der Skandia Navigator dar, der auf 30 Kennzahlen aus den Bereichen Finanzen, Kunden, Prozesse, Mitarbeiter, Entwicklung und Erneuerung basiert (Edvinsson, Malone 1997, 65ff; Sveiby 1998, 254f). Ferner wird die Balance Scorecard (Kaplan, Norton 1996) als strategisches Managementinstrument zur Übersetzung der Unternehmensstrategie herangezogen, das speziell nicht-finanzielle Kennzahlen einbezieht und diese zu finanziellen Größen in Beziehung stellt. Dabei steht diese Methode allerdings nicht dediziert in Bezug zum intellektuellen Kapital, sondern kann um derartige Kennzahlen ergänzt werden.

Diese Ansätze sind dadurch gekennzeichnet, dass die Indikatoren in verschiedenen Ansätzen Anwendung finden, allerdings auch anders interpretiert werden. Ferner ist eine Anpassung der Indikatoren im Hinblick auf Unternehmensbesonderheiten erforderlich, wodurch die Vergleichbarkeit reduziert wird (Dillerup, Ramos 2006, 116ff). Obwohl sich die Scorecard-Methoden nicht zur Ermittlung monetärer

[49] Die Abkürzung steht für ROI of Human Capital.
[50] Siehe hierzu auch Abb. 7 auf Seite 38.

Werte einzelner immaterieller Ressourcen bzw. des gesamten intellektuellen Kapitals eignen, sind ihre Praktikabilität, die mehrperspektivische Betrachtung und die Fokussierung auf die Steuerung positiv hervorzuheben.

2.3.3 Rechnungslegungsstandards

Die Bestrebungen immaterielle Ressourcen zu bewerten, sind auch in die verschiedenen Standards zur Rechnungslegung eingegangen, wobei die Beachtung vergleichsweise spät erfolgte (Arbeitskreis 2001, 989). Die Standardisierungsgremien der Rechnungslegung zielen primär darauf ab, zu identifizieren, wie eine Messung und Bilanzierung immaterieller Ressourcen erfolgen kann.

Im Hinblick auf die Aktivierung in der Bilanz wird in der einschlägigen Literatur dieser Wissenschaftsdisziplin in der Regel der Begriff Vermögenswert verwendet (siehe auch 2.1.2). Immaterielle Vermögenswerte werden in der bilanziellen Praxis als Ressourcen (im Sinne von wirtschaftlichem Vorteil bzw. Nutzen) definiert, die keine gegenständliche Substanz aufweisen und im Unterschied zu finanziellen Ressourcen nicht monetär sind (Küting, Dürr 2003, 1; Helm, Meiler 2004, 390; Möller 2004, 488; Lev 2005, 299). Während zu aktivierten immateriellen Vermögenswerten Pflichtangaben (z.B. im Anlagespiegel) erforderlich sind und weitere in der Regel hoch aggregierte Angaben zu verschiedenen Sachverhalten, wie z.B. Forschungs- und Entwicklungsaufwand, erforderlich sind, so sind detaillierte Angaben zu nicht-aktivierbaren immateriellen Vermögenswerten freiwillig und werden nur von einem Teil der Unternehmen gemacht (Arbeitskreis 2003, 1233)[51]. Nachfolgend werden Unterschiede in der Rechnungslegung nach dem deutschen Handelsgesetzbuches (HGB), den International Accounting Standards (IAS) bzw. International Financial Reporting Standards (IFRS)[52] sowie den U.S. Generally Accepted Accounting Principles (US-GAAP) bezüglich der Aktivierbarkeit immaterieller Ressourcen kurz diskutiert.

HGB: Nach § 266 II HGB werden immaterielle Vermögensgegenstände in drei Gruppen gegliedert: a) Konzessionen, gewerbliche Schutzrechte und ähnliche Rechte b) Geschäfts- oder Firmenwert und c) geleistete Anzahlungen. Für Unternehmen, die nach handelsrechtlichen Vorschriften Rechnung legen, gelten die Aktivierungsvoraussetzungen mit Ausnahme des Aktivierungsverbotes nach § 248 II HGB für selbst erstellte immaterielle Vermögensgegenstände des Anlagevermögens. Gemäß dem Vollständigkeitsgebot nach § 248 I HGB besteht für dem Unternehmen zuordenbare entgeltlich erworbene Vermögenswerte Aktivierungspflicht, sofern diese greifbar, übertragbar und selbständig bewertbar sind (Küting, Dürr 2003, 2). Ferner besteht für selbst erstellte und entgeltlich erworbene immaterielle Vermögensgegenstände des Umlaufvermögens Ansatzpflicht. Das HGB ist durch vorsichtige Bilan-

[51] Siehe hierzu auch Abschnitt 2.3.4.

[52] In 2001 erfolgte die Umbenennung von IASC (International Accounting Standards Committee) zu IASB (International Accounting Standards Board), wobei die IAS von IASC und die IFRS von IASB verabschiedet wurden. Die IAS sind weiterhin gültig.

zierungsgrundsätze gekennzeichnet, wodurch der Umfang der Ertrags- und Vermögenslage in Bezug auf immaterielle Vermögenswerte eingeschränkt wird. Das Deutsche Rechnungslegungs Standards Committee (DRSC) ist im Sinne von § 342 HGB als privates Rechnungslegungsgremium anerkannt, gibt Empfehlungen zur Anwendung der Grundsätze über die Konzernrechnungslegung, berät zur Gesetzgebung und vertritt Deutschland in internationalen Standardisierungsgremien. Um einen immateriellen Vermögensgegenstand ansetzen zu können, muss er nach DRS 12 entgeltlich erworben worden sein, wobei die Empfehlung ausgesprochen wird, das Aktivierungsverbot nach § 242 II HGB aufzuheben, um eine Annäherung an die internationale Rechnungslegung zu erreichen (DRS 12, Anhang A2) (Reich 2006, 20ff).

IAS / IFRS: Zur internationalen Vergleichbarkeit der Rechnungslegung wurden durch das International Accounting Standards Board (IASB) bzw. Committee (IASC) Standards definiert. Die Europäische Union verpflichtet kapitalmarktorientierte Unternehmen, die Jahresabschlüsse nach IFRS zu veröffentlichen. Für die Ansetzbarkeit nach IAS besteht die Voraussetzung, dass ein immaterieller Vermögenswert gemäß der Definitionen (IAS 38.8-38.17) vorliegt und die Ansatzkriterien erfüllt sind (IAS 38.21-38.23). Dies bedeutet im Wesentlichen, dass die Tatbestände Identifizierbarkeit, Beherrschung und künftiger wirtschaftlicher Nutzen sowie Bewertbarkeit erfüllt sein müssen. Im Hinblick auf die Identifizierbarkeit besteht die Voraussetzung, dass der immaterielle Vermögenswert separierbar ist und aus vertraglichen oder anderen gesetzlichen Rechten entsteht (IAS 38.11-12), um ihn vom originären Goodwill abgrenzen zu können[53] (Küting, Dürr 2003, 3). Beherrschung liegt vor, wenn das Unternehmen sich den künftigen wirtschaftlichen Nutzen verschaffen und den Zugriff Dritter auf diesen Nutzen beschränken kann (IAS 38.13). So werden beispielsweise Fähigkeiten von Arbeitnehmern (IAS 38.15) vom Unternehmen nicht beherrscht. Bei Marktkenntnissen oder technischen Erkenntnissen (IAS 38.14) sowie bei Kundenbeziehungen (IAS 38.16) ist ein gesetzlicher Rechtsanspruch Voraussetzung für die Beherrschung. Der künftige wirtschaftliche Nutzen kann Erlöse aus dem Verkauf von Produkten oder der Erbringung von Dienstleistungen, Kosteneinsparungen oder andere Vorteile, die sich für das Unternehmen aus der Eigenverwendung des Vermögenswertes ergeben, beinhalten (IAS 38.17). Dabei ist die Wahrscheinlichkeit heranzuziehen, zu der ein Vermögensgegenstand zu zukünftigen Cash-Flows beiträgt (Rodgers 2003, 184). Zudem hat die Bewertung auf der Basis vernünftiger und begründeter Annahmen zu erfolgen (IAS 38.22). Im Hinblick auf die Bewertbarkeit sind die Anschaffungs- oder Herstellungskosten des Vermögenswertes verlässlich zu bewerten (Reich 2006, 42ff).

US GAAP: Nach der US-amerikanischen Rechnungslegung werden immaterielle Werte vergleichsweise umfassender berücksichtigt. Voraussetzung für die Aktivierbarkeit ist die Erfüllung der Asset-

[53] Der Goodwill bezeichnet die Differenz aus dem Ertragswert bzw. dem Kaufpreis (im Falle des Unternehmenserwerbes) und dem Nettosubstanzwert. Dabei wird zwischen originären, also selbst geschaffenem, und derivativem, also entgeltlich erworbenem Goodwill, unterschieden (Walde 2004, 148).

Definition nach SFAC 6. Demnach muss der Wert zuverlässig schätzbar und der künftige wirtschaftliche Nutzen wahrscheinlich sein (Küting, Dürr 2003, 2). Im Gegensatz zum HGB sind auch selbst erstellte immaterielle Vermögenswerte des Anlagevermögens aktivierbar, wobei umfassende Voraussetzungen für deren Aktivierung erfüllt werden müssen. Nach SFAS 142 sind eine begrenzte Nutzungsdauer und die eindeutige Identifizierbarkeit im Sinne von Abgrenzbarkeit und Einzelbewertbarkeit vorausgesetzt, wobei sich durch letztgenannte Ermessenspielräume ergeben, aufgrund derer von einem Ansatzwahlrecht ausgegangen werden kann (Küting, Dürr 2003, 2).
Ein Vergleich der verschiedenen Rechnungslegungsnormen zeigt auf, dass die Aktivierbarkeit immaterieller Ressourcen nach HGB geringer ausfällt als nach den internationalen Vorschriften US-GAAP und IFRS, was auf die vorsichtigen Bilanzierungsgrundsätze des HGB zurückzuführen ist. Zusammenfassend kann festgestellt werden, dass von der Vielzahl immaterieller Ressourcen über die ein Unternehmen verfügt, nur ein kleiner Teil im Rahmen der Rechnungslegung aktivierbar ist. Ein großer Teil wissensbezogener Ressourcen (z.B. Humankapital) sind von der Bilanzierung ausgenommen, da Unternehmen keine uneingeschränkte Verfügungsmacht haben, der zukünftige wirtschaftliche Nutzen schwer nachweisbar ist sowie intersubjektiv nachprüfbare Bewertungsverfahren fehlen (Persch 2003, 326). Pflichtangaben zu nicht aktivierten immateriellen Ressourcen müssen nur in geringem Ausmaß gemacht werden. So ist beispielsweise nach IAS 38.115 die Summe der Forschungs- und Entwicklungsausgaben anzugeben. Derartige Angaben sind bei handelsrechtlicher Rechnungslegung nach §289 II Nr.3 HGB auch im Lagebericht erforderlich.

2.3.4 Freiwillige Berichterstattung

In den vorangegangenen Abschnitten wurde aufgezeigt, dass ausgehend vom Ansatz des intellektuellen Kapitals verschiedene Ansätze zur Bewertung immaterieller Ressourcen bestehen, die jeweils Vor- und Nachteile aufweisen. Die Aktivierungsfähigkeit variiert über die verschiedenen Rechnungslegungsstandards hinweg. Da immaterielle Ressourcen, die nicht im Sinne der Rechnungslegungsvorschriften bilanzierbar sind, dennoch eine hohe Bedeutung für das Management und die Stakeholder haben können, besteht die Möglichkeit im Rahmen der freiwilligen externen Berichterstattung,[54] zusätzliche Informationen über diese Ressourcen zum Geschäftsbericht zu kommunizieren. Darüber hinaus wirkt sich auch die Vergangenheitsorientierung der Bilanzierungssysteme negativ aus und lässt nur geringe Schlüsse auf zukünftige Entwicklungen zu (Rodgers 2003, 181). Neben einer externen Fokussierung kann die Berichterstattung auch unternehmensintern zum gezielten Umgang mit werthaltigen wissensbezogenen Ressourcen beitragen. Dieser Beitrag kann z.B. in der Erhöhung des Be-

[54] Die Berichterstattung zu immateriellen Ressourcen kann als ein Teil des Value Reportings verstanden werden, das zum Ziel hat, die Differenzen zwischen bilanziellem Eigenkapital, Börsenkapitalisierung und Unternehmenswert zu erklären und somit die Informationsasymmetrien zwischen Management und Investoren zu reduzieren (Arbeitskreis 2002, 2337).

wusstseins für immaterielle Werte und der verbesserten Transparenz gesehen werden, die z.B. in einer SWOT Analyse[55] spezifiziert werden kann (EU 2006; Kraft 2006, 60; Nagel 2006, 479). Im Hinblick auf den Untersuchungsgegenstand Wissensrisiken können diese Ansätze Anhaltspunkte für die Bewertung wissensbezogener Ressourcen liefern. Daher werden im Folgenden die Ziele dieser Berichterstattung und verschiedene Ansätze näher betrachtet. Diese Erkenntnisse werden dann zusammen mit den Verfahren der zuvor dargestellten Bewertungsansätze bzw. Bilanzierungsrichtlinien in Abschnitt 2.3.3 in Bezug auf wissensbezogene Ressourcen integriert betrachtet. Bereits seit Anfang der 90'er Jahre wird das Ziel einer umfassenden Berichterstattung zu nicht aktivierbaren immateriellen Ressourcen von Unternehmen aus dem skandinavischen Raum (z.B. Skandia und Celemi International) verfolgt, die auch verschiedene Bewertungsansätze (z.B. Intangible Asset Monitor) einsetzen (siehe 2.3). Im Rahmen der externen Berichterstattung werden zunehmend Standards eingesetzt, um die Vergleichbarkeit bzw. das Benchmarking zwischen Unternehmen zu verbessern (Mertins et al. 2006, 21ff; Nemetz 2006, 13ff)[56]. So bestehen seitens des Financial Accounting Standards Boards (FASB) seit 2001 Bestrebungen[57], die freiwillige Berichterstattung über nicht aktivierbare immaterielle Ressourcen zu verbessern und einen entsprechenden Standard zu entwickeln. Erste Empfehlungen zielten beispielsweise auf die Angabe der Klassen immaterieller Ressourcen, deren Anschaffungs- bzw. Herstellungskosten sowie deren Werte ab (FASB 2001, 111f).

[55] Siehe hierzu auch Abschnitt 2.1.1.
[56] Das EU-Projekt Intellectual Capital Statement – Made in Europe (InCaS) befasst sich mit der Standardisierung.
[57] Als Beispiel ist das Projekt „Disclosure about Intangible Assets" anzuführen. Siehe auch http://www.fasb.org/project/intangibles.shtml.

Auch der Arbeitskreis „Immaterielle Werte im Rechnungswesen“ betont, dass die Informationslage in Bezug auf den Stand und die Entwicklung immaterieller Ressourcen besonders in Branchen[58], in denen immateriellen Ressourcen eine hohe Bedeutung zukommt, unzureichend ist und hat deshalb einen Vorschlag zur Gestaltung der freiwilligen externen Berichterstattung entwickelt (Arbeitskreis 2003, 1233ff)[60]

Kategorie	Beispiele für Indikatoren
Innovationskapital	• Forschungs- und Entwicklungsausgaben (Gesamtausgaben, Verhältnis zum Umsatz; Informationen zur Streuung, Konzentration der Ausgaben) • Portfolio von Patenten und ähnlichen Schutzrechten (Zahl, Zusammensetzung und Laufzeiten) • Neuproduktrate (Anteil der in den letzen drei Jahren eingeführten Produkte am Gesamtumsatz)
Humankapital	• Fluktuation (Zahl der Mitarbeiter, die das Unternehmen verlassen haben, in Relation zur Gesamtmitarbeiteranzahl) • Weiterbildung (Weiterbildungsausgaben pro Mitarbeiter, Weiterbildungstage pro Mitarbeiter) • Mitarbeiterqualifikation (Anteil der Mitarbeiter mit Ausbildung, Hochschulabschluss, Promotion, Zertifizierung)
Kundenkapital	• Kundenzufriedenheit (Angabe der Methode auf deren Basis die Kundenzufriedenheit ermittelt wurde) • Kundenqualität (Kundenbindungsdauer, Wiederkaufrate, Großkundenanteil) • Marktanteil (Umsatz- bzw. stückbezogene Anteile pro Produkt)
Lieferantenkapital	• Lizenzen (Zahl und Struktur erhaltener Lizenzen als Lizenznehmer) • Schlüssellieferanten (Lieferantenbindungsdauer) • Wertschöpfungstiefe (z.B. Materialaufwand, zugekaufte Dienstleistungen)
Investorenkapital	• Bedeutung bei Analysten (Analystenberichte) • β-Faktor am Eigenkapital-Markt • Bonität am Fremdkapital-Markt
Prozesskapital	• Schnelligkeit der Prozessabläufe (Durchlaufzeit, Liefertreue, Lieferzeit) • Prozessqualität (Kennzahlen zur Messung der Prozessqualität z.B. First pass yield) • Produktqualität (Rückweisquote je Produkt, Beschwerdequote je Produkt, Gewährleistungsaufwände)
Standortkapital	• Standortqualität • Medienpräsenz • Arbeitsmarktattraktivität (z.B. Ranking als potentieller Arbeitgeber bei Hochschulabsolventen)

Tab. 1 Indikatoren zu immateriellen Ressourcen[59]

Dieser Vorschlag legt im Wesentlichen die in Abschnitt 2.3.1 dargestellten Kategorien des intellektuellen Kapitals zugrunde, wobei seitens des Arbeitskreises aus Gründen der Komplexitätsreduktion auf eine Hierarchisierung der einzelnen Komponenten verzichtet wurde und weitere Komponenten wie Investoren- und Standortkapital ergänzt wurden (Arbeitskreis 2001, 990). Als erweiterte Kategorie umfasst das Investorenkapital immaterielle Werte, die sich in günstigen Konditionen zur Eigen- und Fremdkapitalbeschaffung niederschlagen, während letztgenannte Kategorie Standortvorteile berücksichtigt. Für jede der sieben Kategorien werden durch den Arbeitskreis eine Reihe von Kennzahlen vorgeschlagen, die im Rahmen der freiwilligen Berichterstattung Teil des Geschäftsberichts sein können.

In Tab. 1 sind die Kategorien der immateriellen Werte dargestellt und Beispiele für Kennzahlen aufgeführt. Im

[58] Siehe hierzu auch die Überlegungen zur Wissensintensität in Abschnitt 2.2.6.

[59] Indikatoren basieren auf dem Arbeitskreis „Immaterielle Werte im Rechnungswesen“ (Arbeitskreis 2003, 1236f)

[60] Mögliche Orte der Berichterstattung sind nach dem Arbeitskreis „immaterielle Werte“ Anhang, Lagebericht, Management’s Discussion and Analysis (MD&A), Operating & Financial Review (OFR) oder ein separater Teil des Geschäftsberichts (Arbeitskreis 2003, 1234).

Hinblick auf die in Abschnitt 2.2.3 erläutert wissensbezogenen Ressourcen sind insbesondere die Kategorien Human-, Prozess- und Innovationskapital von Bedeutung. Ersteres betrifft an Personen gebundenes Wissen, wobei v.a. die Mitarbeiterqualifikation und die Weiterbildungstage einen Anhaltspunkt über den Wert der korrespondierenden Ressourcen geben. Für organisatorisch verankertes Wissen (siehe Abschnitt 2.2.3) sind insbesondere Kennzahlen des Prozesskapitals von Relevanz, da sie beispielsweise im Unternehmen implementierte Best Practices zu spezifischen Abläufen zu anderen Unternehmen in Bezug setzen. Im Hinblick auf in Objekten inkorporiertes Wissen können Anhaltspunkte zur Ermittlung der entsprechenden Werte durch Kennzahlen des Innovationskapitals gewonnen werden. So kann die Neuproduktrate Aufschluss über den Erfolg der Inkorporierung von Wissen geben, während auch die Anzahl der Patente und insbesondere deren Zitation Erkenntnisse über deren Wert liefern können. Als weiteres Instrument im Kontext der freiwilligen Berichterstattung haben in den letzten Jahren Wissensbilanzen in Unternehmen und Organisationen Verbreitung gefunden. Dabei setzen insbesondere Universitäten oder Unternehmen mit einem hohen Forschungs- und Entwicklungsanteil dieses Instrument ein, um Transparenz über ihr intellektuelles Kapital und dessen Entwicklungen zu gewinnen.

Pioniere im Hinblick auf die Veröffentlichung der Wissensbilanzierung waren dabei die Forschungsorganisation Austrian Research Center (ARC) und das Deutsche Luft- und Raumfahrtzentrum (DLR) (Leitner 2003, 20)[61]. Zur Wissensbilanzierung bestehen verschiedene Grundmodelle, die unterschiedlichen Forschungsprojekten entstammen[62] und zumeist Ähnlichkeiten in Bezug auf die Kennzahlenkategorien aufweisen, wobei in diesem Kontext das Modell des ARC herangezogen wird (siehe Abb. 8).

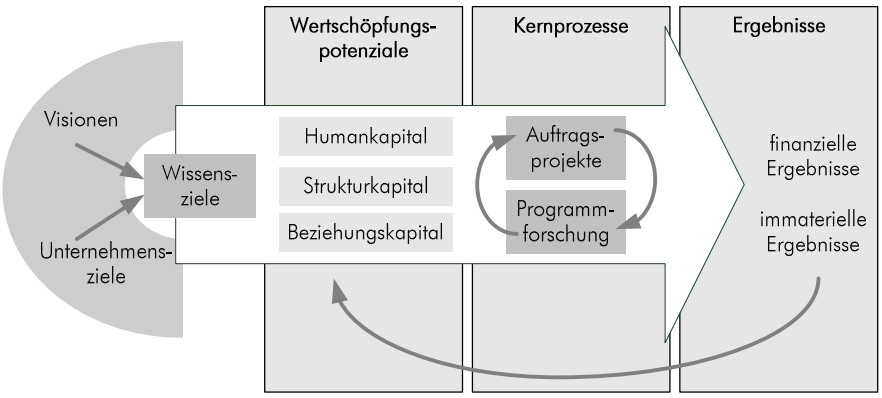


Abb. 8 Modell der Wissensbilanz nach ARC

Nach diesem prozessorientierten Modell werden durch die Wissensziele, die aus den Unternehmenszielen und den Visionen abgeleitet werden, die Rahmenbedingungen vorgegeben. Darauf basierend werden die Wertschöpfungspotentiale ausgewiesen, die in die Elemente Human-, Struktur- und Beziehungskapital[63] untergliedert sind und somit

[61] Das ARC 1999 erstellt seit 1999 und das DLR seit 2000 eine Wissensbilanz.
[62] Siehe hierzu Meritum (siehe www.uam.es/meritum), Wissensbilanz Made in Germany (BMWI 2006), Ricardis (EU 2006) und (Dillerup, Göttert 2005).
[63] Siehe hierzu auch Abschnitt 2.3.1.

mit dem Grundmodell des intellektuellen Kapitals (siehe Abschnitt 2.3.1) korrespondieren.

Zusätzlich werden Kennzahlen zu den Kernprozessen ausgewiesen (siehe Abb. 8). In diesem Fall bestehen entsprechend der Ausrichtung der Unternehmen Unterschiede. Als Aggregat der Wissensbilanzierung werden die finanziellen und die immateriellen Ergebnisse angegeben. In Tab. 2 sind beispielhafte Kennzahlen im Hinblick auf die Wertschöpfungspotentiale und die Ergebnisse der Wissensbilanz zusammengefasst (DLR 2001; ARC 2005). Im Bereich des Humankapitals, das im Hinblick auf wissensbezogene Ressourcen mit der Kategorie Personen korrespondiert, können als Kennzahlen zur Bewertung z.B. der Anteil an Wissenschaftlern in Prozent sowie deren durchschnittliche Betriebszugehörigkeit in Jahren, die Erfahrungswissen widerspiegelt, herangezogen werden. Darüber hinaus können Zu- und Abflüsse an Humankapital durch Fluktuationsstatistiken unter Einbezug der Berufserfahrung abgebildet werden. Hinsichtlich Weiterbildung können die durchschnittlichen Weiterbildungstage bzw. -kosten je Mitarbeiter zugrunde gelegt werden, um Investitionen in Humankapital abzubilden.

Kategorie	Beispiele für Indikatoren
Humankapital	• Anteil Wissenschaftler • durchschnittliche Betriebszugehörigkeit in Jahren • Weiterbildungstage • durchschnittliche Weiterbildungskosten • Anzahl Mentoring-Paare • eingereichte betriebliche Verbesserungsvorschläge
Strukturkapital	• Anzahl neuer Projekte • Anzahl Zertifizierungen und Akkreditierungen • Trefferquote bei Ausschreibungen zu Forschungsprojekten • IT-Ausgaben je Mitarbeiter • Zufriedenheit mit der IT-Unterstützung
Beziehungskapital	• Forschungstätigkeit im Ausland / Auslandsabordnungen • Anzahl Gastforscher • Anzahl Vorträge • Anzahl Teilnahme an Gremien
Ergebnisse	• Anzahl Patente • Anzahl Publikationen

Tab. 2 beispielhafte Indikatoren der Wissensbilanz[64]

Weiterhin kann die Anzahl von Mentoring-Paaren in Relation zur Anteil neuer Mitarbeiter einen Eindruck zur Güte der Einarbeitung und des Wissensaustausches geben, während die Anzahl eingereichter betrieblicher Verbesserungsvorschläge Aufschlüsse über die Innovationsfähigkeit der Mitarbeiter gibt. Im Hinblick auf die Bewertung des Strukturkapitals können beispielsweise die Anzahl neuer Projekte sowie die Anzahl an Zertifizierungen und Akkreditierungen herangezogen werden. Zusätzlich kann noch die der Erfolg der Projektakquisition beachtet werden. In Bezug auf die IT können die Ausgaben je Mitarbeiter und deren Zufriedenheit mit der IT in die Wissensbilanz einbezogen werden. Beziehungskapital spiegelt im Kontext der Wissensbilanz die Vernetzung wider und schließt beispielsweise die Dauer von Forschungsaufenthalten im Ausland, die Anzahl an Gastforschern, die Anzahl an Vorträgen oder die Teilnahme an Gremien ein. Die Ergebnisse der Wissensbilanz stellen eine Aggregation dar, die Kennzahlen aus den Wertschöpfungspotentialen eventuell erneut aufgreift. So können neben diesen Ergeb-

[64] Die Beispiele basieren auf den Wissensbilanzen des ARC (2005) und des DLR (2001).

nissen insbesondere auch die Anzahl an Patenten und die Publikationen als Ergebnisse angeführt werden[65].

Nach der Analyse der verschiedenen Bewertungsmöglichkeiten im Kontext der Bewertungsansätze, Rechnungslegungsstandards und der freiwilligen Berichterstattung wird in folgendem Abschnitt eine integrierte Betrachtung unter Einbezug der Kategorisierung wissensbezogener Ressourcen vorgenommen.

2.3.5 Integrierte Betrachtung der Bewertung wissensbezogener Ressourcen

Die vorhergehende Betrachtung der verschiedenen Bewertungsansätze im Kontext immaterieller Ressourcen haben deutlich gemacht, dass zum Teil erhebliche Bewertungsprobleme bestehen, die zur Folge haben, dass im Kontext der Bilanzierung, die unabhängig vom zugrunde gelegten Standard tendenziell eher vorsichtig erfolgt, nur wenige dieser Ressourcen aktivierungsfähig sind. Dennoch können für die Bewertung wissensbezogener Ressourcen einige wertvolle Anhaltspunkte gewonnen werden.

Der in Abschnitt 2.3.1 dargelegte Ansatz zum intellektuellen Kapital dient dabei als grundlegendes Modell für die verschiedenen Bewertungsansätze, die auf Basis dieser Struktur entsprechende Indikatoren zugrunde legen. In Bezug auf wissensbezogene Ressourcen (siehe Abschnitt 2.2.3) korrespondiert an Personen gebundenes Wissen mit der Kategorie Humankapital. Strukturkapital verteilt sich auf die beiden anderen Dimensionen, die in Objekten inkorporiertes und organisatorisch verankertes Wissen bezeichnen.

Die in Abschnitt 2.3.2 dargestellten Bewertungsansätze liefern zum Teil Anhaltspunkte zur Bewertung wissensbezogener Ressourcen, wobei Marktkapitalisierungsmethoden sich für eine Einzelbewertung nicht eignen, da sie auf einer sehr grob granularen Ebene den gesamten Wert immaterieller Ressourcen in der Regel als Residualgröße ermitteln. Direkte Methoden hingegen eignen sich besser, da sie auf einzelne wissensbezogene Ressourcen abstellen. Dabei können die Methoden zur Bewertung von Patenten übertragen werden. In Bezug auf ROA Methoden können spezifische Kennzahlen wie der HCROI zur Bewertung des Humankapitals verwendet werden. Diese Kennzahl setzt dabei den Gewinn und die Humankapitalkosten zueinander in Beziehung, wobei auch Fluktuationsraten Eingang finden. Da Scorecard Methoden auf Indikatoren basieren, eigen sich diese Bewertungsverfahren besonders gut. So werden z.B. im Intangible Asset Monitor nach Sveiby (1996) verschiedene Indikatoren zur Messung der internen und externen Struktur herangezogen. Hinsichtlich der verschiedenen Bilanzierungsansätze kann in Bezug auf die Bewertung wissensbezogener Ressourcen abgeleitet wer-

[65] Die Wissensbilanz dürfte sich v.a. im Bereich der Hochschulen und forschungsfokussierten Institute bzw. Unternehmen weiter etablieren. So sind an österreichischen Universitäten 20% der Budgetvergabe von der Wissensbilanz abhängig (Mosch 2005, 3).

den, dass in bestimmten Fällen Anschaffungs- bzw. Herstellungskosten zugrunde gelegt werden. Diese Verfahren können z.B. bei dokumentiertem Wissen oder Patenten herangezogen werden, indem die erforderliche Erstellungszeit eingerechnet wird.

Ein ähnliches Vorgehen wie die in Abschnitt 2.3.2.4 kurz erläuterten Scorcard Methoden weisen auch die Ansätze zur freiwilligen Berichterstattung (siehe Abschnitt 2.3.4) auf. Aus diesem Grund werden für die nachfolgende integrierte Betrachtung insbesondere diese Ansätze herangezogen. Auf der Basis der in Abschnitt 2.2.3 entwickelten Kategorisierung von wissensbezogenen Ressourcen werden im Folgenden je Wissensträger einige relevante Kennzahlen zur Bewertung wissensbezogener Ressourcen erläutert. Dabei erhebt diese Betrachtung nicht den Anspruch auf Vollständigkeit, sondern soll vielmehr aufzeigen, wie wissensbezogenen Ressourcen der drei Kategorien ein Wert zugewiesen werden kann, um auf dieser Basis gezielte Risikobetrachtungen vornehmen zu können. Im Projekt Ricardis erfolgt eine Dreiteilung der jeweiligen Kennzahlen. So werden auf der einen Seite Investitionen betrachtet, die dazu beitragen sollen, den Wert der Ressourcen zu erhöhen. Zum Zweiten wird der Wert bzw. die Anzahl der Ressourcen selbst im Sinne einer Bezugsgröße betrachtet. Zum Dritten werden die Effekte der Investitionen betrachtet, zu deren Ermittlung in der Regel die Bezugsgröße zugrunde gelegt wird (EU 2006, 88f). Diese Einteilung liegt auch Tab. 3 zugrunde, die die Basis für die nachfolgenden Erörterungen darstellt.

	Personen	**Organisation**	**Objekt**
Investitionen	• Weiterbildungsaufwand • Mentoring Paare • Mitarbeiterbindung • Rekrutierungsausgaben	• Erstellungsaufwand für Lessons Learned / Best Practices • Investitionen in IT • Investitionen in Konferenz- und Workshopteilnahmen	• Investitionen in Forschung und Entwicklung • Anzahl beantragter Patente • Anzahl beantragter Projekte • Anzahl erstellter Angebote • Anzahl erstellter Publikationen
Ressourcen / Bezugsgröße	• Anzahl der Mitarbeiter • Ausbildungsgrad (Anteil) • Berufserfahrung im Unternehmen (Anteil)	• Beziehungen zu Partnern • Anzahl Lessons Learned / Best Practices	• Anzahl Patente • Anzahl Zertifizierungen • Anzahl Produkte • Anzahl Projekte • Anzahl Publikationen
Effekte	• Mitarbeiterzufriedenheit • Fluktuationsrate • Gewinn je Mitarbeiter • HCROI • Wertschöpfungsbeitrag je Mitarbeiter	• Anzahl angewandter Lessons Learned / Best Practices • Kundenzufriedenheit • Anzahl neuer Beziehungen • Anzahl betrieblicher Verbesserungsvorschläge	• Neuproduktrate • Umsatzanteil neuer Produkte / Projekte • erfolgreiche Patentierungen • erfolgreiche Projektakquisitionen • erfolgreiche Auftragsakquisitionen

Tab. 3 Indikatoren zur Bewertung wissensbezogener Ressourcen

Wissensbezogene Ressourcen der Kategorie Person: Unter der Kategorie Personen werden die Mitarbeiter des Unternehmens subsumiert, die in verschiedenen Themengebieten Kompetenzen und Erfahrungen aufweisen sowie mit anderen Mitarbeitern, Kunden, Lieferanten und Partnern in Beziehung stehen. Zur Bewertung der Investitionen können exemplarisch folgende Kennzahlen herangezogen

werden. Investitionen in die Weiterbildung der Mitarbeiter haben zum Ziel, den Wert des Humankapitals zu erhöhen und die Produktivität der Mitarbeiter zu verbessern. Zur Bestimmung des Investitionsaufwands können auf der einen Seite Zeitbedarf der Weiterbildung und auf der anderen Seite die Kosten der Weiterbildung selbst veranschlagt werden (Sveiby 1996; Arbeitskreis 2003, 1233ff; EU 2006, 89). Beide Größen lassen sich monetär bewerten. Als spezielle Form der Weiterbildung, die primär auf die Übertragung von Erfahrungswissen abstellt, können Mentoring-Paare im Unternehmen eingesetzt werden, bei denen einem neu rekrutierten Mitarbeiter ein erfahrener Mitarbeiter zur Seite gestellt wird (Liebowitz, Suen 2000, 63). Zusätzlich zu Weiterbildungsaufwendungen sind auch Investitionen in die Mitarbeiterbindung von Relevanz und fokussieren primär darauf, den Bestand des Humankapitals zu erhalten. Das Ziel besteht darin, durch verschiedene Maßnahmen, wie z.B. komparative Vergütung oder Anreizsysteme, das akquisitorische Potential des Unternehmens zu erhöhen und somit die Wahrscheinlichkeit der Abwanderung von Mitarbeitern zu reduzieren. Neben Investitionen in die Weiterbildung entstehen auch Aufwendungen im Kontext der Beschaffung neuer Mitarbeiter, die möglicherweise über knappe Qualifikationen verfügen (EU 2006, 89).

Als generelle Bezugsgröße im Kontext wissensbezogener Ressourcen der Kategorie Personen kann die Anzahl der Mitarbeiter herangezogen werden, auf deren Basis verschiedene Anteile errechnet werden können. So kann ein Anteil das Qualifikationsniveau der Mitarbeiter einbeziehen, da es maßgeblich den Wert für das Unternehmen beeinflusst[66]. Das Qualifikationsniveau kann z.B. eine Ausbildung, ein Studium, eine Promotion sowie Zertifizierungen betreffen. Dabei wird der Wert entscheidend durch die Verfügbarkeit der entsprechenden Qualifikationen auf dem Arbeitsmarkt beeinflusst. Verfügen die Mitarbeiter beispielsweise über knappe Qualifikationen, wie z.B. spezifisches Ingenieurwissen, so nimmt deren Wert zu. Auf Basis der Bezugsgröße lässt sich der Anteil hoch qualifizierter Mitarbeiter bestimmen, wobei sich eine derartige Relation auch auf spezifische Qualifikationen beziehen kann (Sveiby 1996). Neben dem Ausbildungsgrad stellt die Berufserfahrung im Unternehmen eine Kennzahl dar, die den Wert der Mitarbeiter im Kontext des Humankapitals beeinflusst. Dieser Wert kann daran festgemacht werden, dass Mitarbeiter mit ansteigender Unternehmenszugehörigkeit mit den Strukturen vertrauter sind, über Beziehungsnetzwerke verfügen und somit Effizienzvorteile gegenüber unerfahrenen Mitarbeitern aufweisen (Sveiby 1996).

Neben diesen Kennzahlen sind insbesondere auch die Effekte zu beachten, die aufzeigen, inwiefern sich die Investitionen positiv auswirken. So können derartige positive Auswirkungen der in Humankapital getätigten Investitionen u.a. an der Mitarbeiterzufriedenheit festgemacht werden. Im konkreten Fall betrifft dies Maßnahmen zur Mitarbeiterbindung und zur Weiterbildung. Die Effekte können an der Entwicklung dieses Index über einen längeren Zeitraum hinweg identifiziert werden (Mouritsen et al. 2004, 52; EU 2006, 89). Weiterhin können positive Effekte der Investitionen auch an der Fluktua-

[66] Siehe hierzu auch die Analyse der Wissensintensität in Abschnitt 2.2.6.

tionsrate festgemacht werden. Dabei kann eine zweiseitige Betrachtung vorgenommen werden und sowohl die Stabilität der bestehenden Mitarbeiter als auch der Zuwachs an neuen Mitarbeitern einbezogen werden. Im Hinblick auf die bestehenden Mitarbeiter kann Erfolg dann konstatiert werden, wenn nur eine geringe Anzahl der Mitarbeiter das Unternehmen verlässt, da dies ein Indiz für eine hohe Zufriedenheit ist. Zum anderen spricht eine hohe Erfolgsquote bei hoch qualifizierten Mitarbeitern für die Attraktivität des Unternehmens auf dem Arbeitsmarkt (Sveiby 1996; EU 2006, 89)[67]. Darüber hinaus bestehen verschiedene Ansätze, die Anzahl der Mitarbeiter oder die Humankapitalkosten mit finanziellen Größen wie Gewinn oder Umsatz in Beziehung zu setzen (Fitz-Enz 2003, 53; EU 2006, 89). Sveiby schlägt vor den Wertschöpfungsbeitrag anstelle des Umsatzes oder Gewinns heranzuziehen, da diese Größe vergleichsweise geringer extern beeinflusst wird (Sveiby 1996). Darüber hinaus kann auch der Erfolg der Mentoring-Paare an der Entwicklung der Mitarbeiter gemessen werden (Liebowitz, Suen 2000, 63)[68].

Wissensbezogene Ressourcen der Kategorie Organisation: Wissensbezogene Ressourcen dieser Kategorie betreffen vorwiegend Gruppenwissen und Wissen, das in Strukturen, Routinen und Prozessen inkorporiert ist. Zur Bewertung dieser Ressourcen können exemplarisch die nachfolgenden Kennzahlen herangezogen werden, die analog zur vorherigen Betrachtung in die drei Kategorien Investitionen, Bezugsgröße und Effekte unterteilt und in Tab. 3 abgetragen sind.

Im Hinblick auf die Investitionen kann der Aufwand für die Erstellung von Lessons Learned und Best Practices veranschlagt werden. So werden z.B. im Rahmen von Projekt-Debriefings, Lessons Learned dokumentiert oder Best Practices zur verbesserten Durchführung spezifischer Routinen oder Prozesse entwickelt (Liebowitz, Suen 2000, 63). Darüber hinaus kann die Durchführung von Prozessen und die Anwendung von Wissen entscheidend durch IT-Systeme oder weitere Investitionen unterstützt werden, da sie die Erfüllung spezifischer Aufgaben erleichtern können. In diesem Kontext werden verschiedene Kennzahlen wie IT-Investitionen je Mitarbeiter etc. angegeben (Sveiby 1996; DLR 2001, 22f; ARC 2005, 42). Weitere zeitliche und finanzielle Aufwendungen treten in Zusammenhang mit der Teilnahme bzw. Durchführung von Workshops und Konferenzen auf. Diese Aufwendungen stellen bezogen auf den Ansatz des intellektuellen Kapitals[69] Investitionen in Beziehungskapital dar (Liebowitz, Suen 2000, 63).

Als Bezugsgröße für wissensbezogene Ressourcen der Kategorie Organisation können die Anzahl der verfügbaren Lessons Learned und Best Practices herangezogen werden. Weiterhin kann als Bezugsgröße die Anzahl der Beziehungen zu Partnern zugrunde gelegt werden (Liebowitz, Suen 2000, 63).

---

[67] Bei der Bewertung der Fluktuation sollte das Ausbildungsniveau und die Berufserfahrung durch die Errechnung spezifischer Teilquoten berücksichtigt werden.

[68] Als Vergleichsmaßstab kann hierbei die durchschnittliche Entwicklung von Mitarbeitern ohne Mentoring herangezogen werden.

[69] Siehe hierzu auch Abschnitt 2.3.1.

Im Hinblick auf die Effekte, die widerspiegeln, inwiefern sich die Investitionen auszahlen, stellt die Anzahl erfolgreich angewandter Lessons Learned eine Kennzahl dar (Liebowitz, Suen 2000, 63). Darüber hinaus kann der Effekt der Investitionen an der Kundenzufriedenheit und speziell an deren Entwicklung festgemacht werden. Auch die Rate der Wiederholungskäufe kann in diesem Zusammenhang als Kennzahl herangezogen werden (Sveiby 1996). Zudem zeigt sich der Effekt der Investitionen in Bezug auf den Aufbau des Beziehungskapitals, der im konkreten Fall mit Konferenz- und Workshopteilnahmen korrespondiert, in der Anzahl neuer Beziehungen. Diese können zur verbesserten Durchführung von Aufgaben, Projekten und Prozessen beitragen (Simonin 1999, 597, 621; Liebowitz, Suen 2000, 62; Mouritsen et al. 2004, 52).

Wissensbezogene Ressourcen der Kategorie Objekt: In Objekten inkorporiertes Wissen als dritte Kategorie wissensbezogener Ressourcen umfasst beispielsweise Produkte, Konzepte oder Patente, die unter Einsatz von Wissen entwickelt wurden. Zu deren Bewertung können unter Zugrundelegung der Dreiteilung exemplarisch folgende Kennzahlen herangezogen werden.

Um Wissen in Objekte zu inkorporieren, werden in Unternehmen Investitionen in Forschung und Entwicklung getätigt, die von der Errichtung neuer Produktionsanlagen und die Implementierung neuer Verfahren bis zur Einstellung neuer Mitarbeiter reichen (Sveiby 1996; EU 2006, 89). Diese Aufwände schlagen sich auch in Anträgen zur Patentierung nieder, wobei der personelle Zeitaufwand einzurechnen ist (EU 2006, 89). Weitere Aktivitäten, die als Investitionen gesehen werden können, sind Anträge für Projekte oder erstellte Angebote für Kunden. Zu dieser Kategorie zählen auch Publikationen (Know-Center 2006, 38).

Als Bezugsgröße kann die Gesamtanzahl der Patente, Zertifizierungen, Produkte, Projekte und Publikationen herangezogen werden (Liebowitz, Suen 2000, 63). Die Entwicklung dieser Größen ist relevant, wenn der Effekt der Investitionen bestimmt werden soll. Die Auswirkungen können exemplarisch auf Basis der Neuproduktrate ermittelt werden, die den Erfolg der Investitionen in Forschung und Entwicklung widerspiegelt, indem sie angibt wie viele Produktentwicklungen tatsächlich zu einem Produkt gereift sind (Sveiby 1996). Darüber hinaus kann der Umsatzanteil neuer Produkte z.B. in Bezug auf Produkte, die in den letzten drei Jahren eingeführt wurden, herangezogen werden. Auch dieser Indikator gibt den Erfolg der Investitionen in Forschung und Entwicklung an (Sveiby 1996; EU 2006, 89). Weiterhin kann die Erfolgsrate der Patentierungen, die sich aus der Anzahl der Patentanträge und der Anzahl der genehmigten Patente errechnet, über die Auswirkungen der Investitionen Aufschluss geben. Speziell zur Ermittlung des Wertes des Patentes kann neben den Bewertungsmethoden auch die Anzahl der Patentzitationen einbezogen werden (Hall et al. 2000a, 4ff). Analoges gilt für die Erfolgsrate von Projektanträgen oder Angebotserstellungen.

2.4 Zusammenfassung und Diskussion

In den vorangegangenen Abschnitten wurde ausgehend vom ressourcenbasierten Ansatz das Begriffsverständnis zu Ressourcen dargelegt und eine generische Unterteilung in finanzielle, materielle und immaterielle Ressourcen vorgenommen. Dabei haben insbesondere letztgenannte für den Untersuchungsgegenstand Relevanz, da wissensbezogene Ressourcen eine Teilmenge der immateriellen Ressourcen darstellen. Ausgehend von einem heterogenen Begriffsverständnis zu Wissen liegt dieser Arbeit eine wertschöpfungsfokussierte Sichtweise zugrunde, nach der Wissen als Input bzw. Ressource gesehen wird und zugleich einen Output bzw. ein Produkt darstellt. Dieses Verständnis liegt auch dem wissensbasierten Ansatz zugrunde, nach dem wissensbezogene Ressourcen die zentralen Werttreiber darstellen und dem Unternehmen die Rolle zukommt, diese Ressourcen zu bewirtschaften. Wissensbezogene Ressourcen können anhand verschiedener Dimensionen beschrieben werden, die deren Spezifität, Kontexteinbettung oder den Grad der Explizierung betreffen. Für die Bewirtschaftung ist es ferner erforderlich, dass den Besonderheiten dieser Ressourcen, die sich beispielsweise auf die Transferierbarkeit, die Handelbarkeit oder den Einsatz von Schutzrechten beziehen, Rechnung getragen wird. Die Bewirtschaftung wissensbezogener Ressourcen und somit auch der risikobewusste Umgang sind dabei insbesondere für Unternehmen von Relevanz, deren Aufgaben, Prozesse und Produkte wissensintensiv sind, wobei die Wissensintensität je nach Charakteristika und Positionierung der Unternehmen variiert. Dabei wird im Rahmen dieser Arbeit die Auffassung vertreten, dass Wissensintensität nicht auf bestimmte Branchen reduziert, sondern vielmehr am Grad der Erfüllung bestimmter Kriterien festgemacht werden sollte.

In Bezug auf eine Betrachtung von Wissensrisiken ist die Ermittlung des Wertes der potentiell betroffenen wissensbezogenen Ressourcen von Relevanz, um eine geeignete Informationsbasis für das Management dieser Risiken zu schaffen. Insgesamt zeigt sich, dass die Bewertung immaterieller Ressourcen aktuell noch an ihre Grenzen stößt, da einerseits Bewertungsprobleme in Bezug auf die verschiedenen Verfahren bestehen und andererseits auch aufgrund der durch Vorsichtsprinzipien zu charakterisierenden Rechnungslegungsstandards auch nur ein geringer Anteil dieser Ressourcen in der Bilanz aktivierbar ist[70]. Die integrierte Betrachtung in Abschnitt 2.3.5 hat gezeigt, welche Arten von Kennzahlen speziell für wissensbezogene Ressourcen bestehen. Sie stellen somit einen ersten Anhaltspunkt für die Wertermittlung dar, wobei die Ansätze zur freiwilligen Berichterstattung, die auch die Wissensbilanz einschließen, präferiert herangezogen werden können.

[70] Kaplan und Norton bezeichnen die Wertmessung bei immateriellen Ressourcen daher auch als den „Heiligen Gral der Buchführung“ (Kaplan, Norton 2004, 52).

3 Risiko und Risikomanagement

Nachdem die Bedeutung der Ressource Wissen aufgezeigt wurde, werden in diesem Kapitel die Konzepte Risiko und RM detailliert betrachtet. Dazu werden zunächst verschiedene betriebswirtschaftliche Sichtweisen auf Risiko erläutert und einander gegenübergestellt (3.1). Im Anschluss daran werden verschiedene Risikotypen (3.2) betrachtet und dabei operationelles Risiko (3.3) als spezieller Risikotyp, der auf die Ebene der Geschäftsprozesse ausgerichtet ist, hervorgehoben. Um die Bandbreite der verschiedenen Risiken aufzuzeigen, wird eine Kategorisierung zu Risiken im Allgemeinen und operationellen Risiken im Speziellen erörtert (3.4). Basierend auf einem prozessorientierten Verständnis wird anschließend RM als Disziplin erläutert und dabei auf die relevanten Kern- und Unterstützungsaufgaben eingegangen (3.5). Das Kapitel schließt mit einem kurzen Abriss relevanter Vorschriften zu RM (3.6) und einer Diskussion (3.7).

3.1 Betriebswirtschaftliche Sichtweisen auf Risiko

Bereits beim sprachlichen Ursprung des Wortes Risiko besteht Uneinigkeit, da dessen Herkunft nicht endgültig bestimmt ist. So bedeutet das arabische Wort risc „Schicksal“ bzw. „gegeben von Allah“, während das altgriechische riza „Wurzel“ oder „Klippe“ bedeutet, das vorrömische rixicar „streiten“ oder „widerstreben“ und das spanische risco „Klippe“ (Keller 2004, 62; Norrman, Lindroth 2004, 17f).

Diese Uneinigkeit setzt sich in der betriebswirtschaftlichen Literatur fort, in der bisweilen ebenfalls kein einheitlicher Risikobegriff besteht. Grundsätzlich können Risiken auf den drei Ebenen Gesellschaft, Individuum und Unternehmen betrachtet werden (Peter 2002, 19ff). Während sich erstere aus Ereignissen des gesellschaftlichen und politischen Umfeldes oder aus Naturkatastrophen ergeben und sich Risiken auf der Ebene Individuum beispielsweise auf Existenzbedrohungen oder Krankheiten beziehen, sind in diesem Kontext vorwiegend Unternehmensrisiken von Relevanz. Diese entspringen dabei der Geschäftstätigkeit selbst und betreffen verschiedene Bereiche des Unternehmens, wie z.B. Finanzen oder Personal.

Allgemein ist Risiko im betriebswirtschaftlichen Kontext mit einer Verlustgefahr[71] verbunden, die sich im Rahmen der unternehmerischen Tätigkeit aus der Unsicherheit über den Eintritt von unerwünschten Ereignissen ergibt (Kaplan, Garrick 1981, 12; Kendall 1998, 163; Bitz 2000, 13; Diederichs et al. 2004, 189; Wallmüller 2004, 6). DeLoach führt in diesem Kontext unterschiedliche Ursprünge für Ereignisse, die Risiken auslösen, an. So können einerseits externe Ereignisse wie politische Prozesse, Katastrophen etc. zu Risiken führen oder entsprechend Ereignisse intern im Rahmen der Ausführung der Geschäftsprozesse hervorgerufen werden. Neben dem unbeeinflussbaren Eintritt

[71] Als ein Vertreter der Sichtweise Risiko als Verlustgefahr kann Bussmann angeführt werden (Bussmann 1955, 12).

von Ereignissen, können sich entsprechende Ereignisse auch aus konkreten Entscheidungen also aktivem Handeln ergeben (DeLoach 2000, 50; Krämer 2002a, 232).

In der Literatur zu Risiko und RM erfolgt zum Teil eine Vermengung der Begriffe Risiko, Gefahr und Bedrohung. Um die Trennschärfe für die nachfolgende Diskussion des Risikobegriffs zu gewährleisten, wird folgende Abgrenzung zugrunde gelegt. Eine Gefahr bzw. Bedrohung ist vorhanden und stellt damit eine Quelle für Risiken dar, während Risiko die Möglichkeit des Erleidens eines Verlustes bzw. Schadens bezeichnet. Somit ist bei Risiko nicht das bloße Vorhandensein einer Gefahr, sondern die Wahrscheinlichkeit, dass sich diese in einem Schaden realisiert, von Relevanz (Kaplan, Garrick 1981, 12; Neumann 1995, 23; Peltier 2001, 21). Das Schadensausmaß muss im Kontext der ergriffenen Schutzmaßnahmen gesehen werden, da es von diesen limitiert wird (Kaplan, Garrick 1981, 12).

Innerhalb dieses Grundverständnisses bestehen unterschiedliche Strömungen, die Risiko an Abweichungen festmachen und Risiko mit deren Zunahme ansteigt (Rüsberg, Süchting 1992, 131). Abweichungsbezogene Ansätze zur Definition von Risiko setzten einerseits an den Ursachen des Risikos und andererseits an dessen Auswirkungen an (Piaz 2002, 12; Jonen 2005, 50f). Dabei lassen sich verschiedene Strömungen unterteilen, die sich aus unterschiedlichen Forschungsrichtungen ergeben und Risiko vorwiegend aus einer ziel-, entscheidungs- oder informationsorientierten Perspektive betrachten (Schuy 1989, 13ff; Hermann 1996, 7ff; Knaese 2004, 24). Bei einer zielorientierten Perspektive steht die potentielle negative Zielabweichung im Vordergrund (Nicklisch 1912, 166; KPMG 1998, 6), während bei der entscheidungstheoretischen Sichtweise die Möglichkeit einer Fehlentscheidung zentral ist (Imboden 1983, 45; Mikus 2001, 6f). Aus einer informationsorientierten Perspektive, finden auch unvollständige Informationen bzw. Informationsdefizite in die Risikobetrachtung Eingang (Bitz 2000, 13; Helten, Hartung 2002, 258). Im Hinblick auf Ursachen und Wirkungen kann die entscheidungs- und informationsorientierte Begriffsauffassung als ursachenbezogen eingeordnet werden, während die zielorientierte Sichtweise auf Risiko als wirkungsbezogen angesehen werden kann (Schulte 1997, 11; Piaz 2002, 12). Über diese Strömungen hinweg wird Risiko allgemein als eine positive oder negative Abweichung von geplanten Größen, von Zielen oder Auswirkungen einer Entscheidung angesehen, wobei eine positive Abweichung als Chance zu sehen ist und eine negative Abweichung das Risiko im engeren Sinne darstellt und die Abweichung monetäre Auswirkungen hat (Erdenberger 2001, 13; Meier 2001, 18; Füser et al. 2002, 496; Knaese 2004, 23). Diese drei Strömungen werden nachfolgend erörtert.

3.1.1 Entscheidungsorientierter Risikobegriff

Bei einer entscheidungsorientierten Sichtweise auf Risiko erfolgt eine Fokussierung auf dessen Ursachen und dabei eine Einschränkung auf Fehlentscheidungen. Diese vornehmlich negative Charakterisierung von Risiko stellt dabei das Problem der rationalen Entscheidung in den Vordergrund

(Schorcht 2004, 22). Diese Risikoauffassung ist insbesondere in der entscheidungstheoretischen Betriebswirtschaftslehre vertreten und geht auf die 1944 entwickelten spieltheoretischen Modelle von Neumanns und Morgensterns zurück, in dem Entscheidungen den handlungsbestimmenden Bestandteil darstellen (von Neumann, Morgenstern 1953).

Nach einer entscheidungsorientierten Sichtweise beruht wirtschaftliches Handeln auf Entscheidungen, für die eine Menge an Aktionen bzw. Handlungsmöglichkeiten zur Verfügung stehen und die zukünftig wirken (Karten 1972, 149). Entscheidungssituationen sind dabei dadurch gekennzeichnet, dass verschiedene Alternativen zur Auswahl stehen. Da der Eintritt der Umweltzustände nicht sicher ist, kann der Entscheidungsträger nicht im Voraus sagen, ob die getroffene Entscheidung im Hinblick auf die Zielsetzung optimal ist (Krämer 2002b, 141). Somit sind Entscheidungssituationen durch Unsicherheit geprägt.

Umweltzustände

Handlungsalternativen	z^1	z^2	z^3	z^4	z^j
a^1	e^{11}	…	…	…	e^{1j}
a^2	…	e^{22}	…	e^{24}	…
a^3	…	…	e^{33}	…	…
a^4	…	e^{42}	…	e^{44}	…
a^i	e^{i1}	…	…	…	e^{ij}

Abb. 9 Grundmodell der Entscheidungstheorie

Das Risiko ergibt sich demnach daraus, dass aus den zur Verfügung stehenden Handlungsmöglichkeiten nicht die optimale Alternative ausgewählt wurde und demzufolge eine Fehlentscheidung vorliegt (Wittmann 1959, 189). Das Eintreten des Risikos wird nach dieser Sichtweise auf das Handeln des Entscheidungsträgers zurückgeführt (Schuy 1989, 16). Dabei wird Risiko als Folge einer Entscheidung und die Unsicherheit als eine notwendige, aber nicht hinreichende Bedingung für dessen Entstehung gesehen (Kratzheller 1997, 12).

Zur Erläuterung kann das Grundmodell der Entscheidungstheorie (siehe Abb. 9) herangezogen werden. Demnach bestehen verschiedene Handlungsalternativen (ai), verschiedene Umweltzustände (zj) und entsprechende Ergebnisse (eij). Im Hinblick auf diese Parameter bzw. deren Entwicklung besteht Unsicherheit. Nach dem Zeitpunkt der Entscheidung kann sich diese als Fehlentscheidung herausstellen (Mikus 2001, 6f). Den j Umweltzuständen können hinsichtlich ihres Eintritts zudem objektive bzw. subjektive Wahrscheinlichkeiten zugeordnet werden (Wall 2001, 209). Somit spricht man von Entscheidung unter Risiko. Liegen keine Wahrscheinlichkeiten vor, so wird dies als Entscheidung bei Ungewissheit bezeichnet (Müller 1993, 3814). Unter Ungewissheit lassen sich zum Teil nicht mal die zukünftigen Zustände vollständig angeben (Gleißner 2001, 121).

Als Kritik an dieser Sichtweise kann angebracht werden, dass eine Reduktion des Risikos auf die Handlungen eines Entscheidungsträgers erfolgt und somit Risiken, die sich beispielsweise aus dem Eintritt nicht beeinflussbarer Ereignisse ergeben, nicht berücksichtigt werden (Braun 1984, 25). Dabei kann Risiko auch nicht durch Nicht-Entscheidung vermieden werden, da diese aufgrund der Hand-

lungsrationalität selbst eine Entscheidungsalternative darstellt (Luhmann 1991, 30f; Neumann 1995, 24ff). Nach einem entscheidungsorientierten Verständnis dient der gezielte Umgang mit Risiken der Absorption von Unsicherheiten, indem es bestimmte Handlungen wahrscheinlicher macht als andere (Strulik 2001, 41).

3.1.2 Informationsorientierter Risikobegriff

Nach einer informationsorientierten Sichtweise auf Risiko stellt der Informationszustand die Ursache des Risikos dar. Risiko bezeichnet somit eine spezifische Informationsstruktur, die den Entscheidungen zugrunde liegt (Imboden 1983, 42). Zur Spezifizierung ist die in 3.1.1 bereits erwähnte Unterscheidung zwischen Risiko und Ungewissheit erforderlich, nach der Risiko durch die Zuweisung von Wahrscheinlichkeiten abgegrenzt werden kann. Hinsichtlich der Ermittlung dieser Wahrscheinlichkeiten bestehen jedoch unterschiedliche Sichtweisen, die sich aus abweichenden entscheidungstheoretischen Grundverständnissen ergeben. So fordert eine Gruppe von Autoren nach einer engen Auslegung des Begriffs, dass die Ermittlung der Wahrscheinlichkeiten objektiv erfolgen muss, da bei subjektiver Einschätzung nicht von Risiko, sondern nur von Ungewissheit gesprochen werden kann (Knight 1921, 347f; Oehler, Unser 2002, 10). Nach dieser Auffassung sind solche Situationen durch ein Informationsdefizit gekennzeichnet, das z.B. darauf zurückzuführen ist, dass nicht alle Umweltzustände bekannt sind oder nicht alle Eintrittswahrscheinlichkeiten ermittelt werden können (Oehler, Unser 2002, 11). Die Wahrscheinlichkeitsverteilung ist dann objektiv, wenn deren Zustandekommen intersubjektiv nachvollziehbar ist (Krämer 2002a, 234). Als Kritik dazu wird angeführt, dass Risikoanalysen rein auf Basis objektiver Wahrscheinlichkeitsverteilungen nicht möglich sind, da objektive Wahrscheinlichkeiten selbst auf individuellen Entscheidungen beruhen (Karten 1972, 158ff; Kruschwitz 1980, 803; Hölscher 1987, 5). Eine andere Gruppe von Vertretern, die einer weiteren Auslegung des Begriffs folgt, akzeptiert auch die subjektive Ermittlung von Wahrscheinlichkeiten für die Risikoanalyse. Subjektive Wahrscheinlichkeiten sind abhängig vom individuellen Informationsstand und werden durch Überzeugungen und Erwartungen beschrieben (Gottwald 1990, 1965). Demnach besteht nach einer weiten Sichtweise das Risiko in einem Informationszustand, bei dem den zukünftigen Umweltzuständen mittels statistischer Verfahren oder auf der Basis von Erfahrungswerten subjektive oder objektive Wahrscheinlichkeiten zugewiesen werden können (Hermann 1996, 11).

Informationszustände können im Hinblick auf Vollständigkeit in die Zustände vollständiger, völlig fehlender und partieller Information unterteilt werden (Schuy 1989, 14). Demnach liegt ein Zustand vollständiger Information dann vor, wenn der Zustand und die Entwicklung aller Informationen mit Sicherheit bestimmt werden können. Dazu ist Kenntnis der Zukunft erforderlich. Im Falle völlig fehlender Informationen liegt ein Mangel an Informationen vor, der auch mit dem Begriff „echte Unsicherheit“ umschrieben wird. Der Zustand partieller Information stellt eine Ausprägung zwischen den

beiden extremen Zuständen dar, in dem der Entwicklung der Informationen objektive bzw. subjektive Wahrscheinlichkeiten zugewiesen werden können (Schuy 1989, 14).

Während nach einer informationsorientierten Sichtweise bei der Entscheidungsfindung Unklarheit über mögliche Auswirkungen besteht, betrachtet die entscheidungsorientierte Risikodefinition eine Zielabweichung aufgrund einer Fehlentscheidung. Somit ist die Beziehung zwischen informations- und entscheidungsorientierter Sicht derart, dass fehlende oder mangelnde Informationen die Unsicherheit bei Entscheidungen erhöhen, während deren Verfügbarkeit die Unsicherheit senkt (Ritchie, Brindley 2001, 29ff). Das Informationsdefizit hat allerdings auch zur Folge, dass eines oder mehrere verfolgte Ziele nicht erreicht werden. Daher fordern Helten und Hartung, dass der Risikobegriff die beiden Elemente Informationsdefizit und Finalität enthält (Helten, Hartung 2002, 258). Die Wirkungen von Risiken stehen bei einer zielorientierten bzw. wirkungsbezogenen Risikoauffassung, die Gegenstand des nächsten Abschnittes (3.1.3) ist, im Vordergrund.

3.1.3 Zielorientierter Risikobegriff

Die entscheidungsorientierte Sichtweise stellt darauf ab, dass Entscheidungsträger aus den zur Verfügung stehenden Alternativen nicht die zur Zielerreichung optimale Entscheidung treffen und betont somit die Beeinflussung durch eigenes Handeln. Neben Fehlentscheidungen können sich Risiken allerdings auch aus dem Eintritt unerwünschter Ereignisse ergeben und so nach einer engen Auslegung des Risikobegriffs zu negativen Abweichungen und damit verbundenen Verlusten führen. Die wirkungsbezogenen bzw. zielorientierten Risikobegriffe stellen nicht auf die Entscheidung als Ursache der Zielverfehlung ab, sondern betonen die Möglichkeit der Zielverfehlung, also die Wirkung auf den Zielerreichungsgrad (Krämer 2002a, 273; Kremers 2002, 13).

Dabei variiert das Begriffsverständnis von der Abweichung von Plan- und Istdaten (Bussmann 1955, 12; Eucken 1965, 141) bis hin zur Sichtweise auf Risiko als Summe der Möglichkeiten, dass sich die Erwartungen des Unternehmens nicht erfüllen (Haller 1986, 18). Der Kern dieser Sichtweise besteht darin, dass ein Zielwert unter einem erwarteten Sollwert liegt und daraus ein wirtschaftlicher Nachteil bzw. Verlust entsteht. Dabei ist das Risiko nicht in der realisierten Zielverfehlung zu sehen, sondern besteht bereits in der Gefahr, dass diese eintritt (Hermann 1996, 8).

Zentral für diese Begriffsauffassung ist, dass der Einbezug einer individuellen Zielsetzung erforderlich ist, da Unternehmen unterschiedliche Ziele verfolgen und auch die Verfehlungen unterschiedlich beurteilen (Happel, Liebewein 2000, 2). Diese Zielsetzungen lassen sich dabei anhand verschiedener Dimensionen wie Inhalt, Ausmaß oder zeitlicher Bezug spezifizieren (Schuy 1989, 18f). Dabei erfolgt durch die Dimension Inhalt eine Spezifizierung, ob es sich beispielsweise um einen Kapitalverlust, einen Wertverlust, eine Kostenerhöhung oder einen Gewinnentgang handelt. Zudem können auch immaterielle Werte, wie z.B. der Firmenwert, betroffen sein, wobei eine quantitative Erfassung dieser

Auswirkungen nicht bzw. nur schwer möglich ist (Oberparleiter 1930, 97). Das Ausmaß bzw. die Intensität der Zielverfehlung kann mittels objektiver oder subjektiver Bewertungsmaßstäbe bestimmt werden. Der Zeitbezug als weitere Dimension dient dazu, zu spezifizieren, bis wann die Ziele erreicht werden sollen. Dabei können Risiken in Bezug auf die Zielerreichung in kurz-, mittel- und langfristig unterteilt werden (Heinen 1966, 119ff).
Der Grad der Zielverfehlung kann dabei absolut und relativ beschrieben werden, während erstere mit einer Nichterreichung des Ziels gleichzusetzen ist und eine relative Abweichung eine Verfehlung in einem bestimmten Ausmaß bezeichnet (Schuy 1989, 19).

3.1.4 Diskussion

Auch wenn vielfach eine isolierte Betrachtung der Strömungen konstatiert wird, so sind die Zusammenhänge doch von Relevanz und die Sichtweisen als komplementär zueinander zu sehen (Schulte 1997, 13). So werden Risiken durch unbeeinflussbare Ereignisse oder durch Ereignisse als Folge des Handelns z.B. das Treffen oder Nichttreffen einer Entscheidung hervorgerufen. Dabei beeinflusst der Informationszustand die Unsicherheit der Zuordnung objektiver oder subjektiver Wahrscheinlichkeiten. Die Risiken wirken sich dann eventuell in einer Zielverfehlung aus, die im Falle einer engen Sichtweise auf Risiko mit Verlusten verbunden ist. Verluste können zudem unabhängig von Zielsetzungen eintreten. Dabei werden Risiken von den jeweiligen Betrachtern subjektiv eingeschätzt. Zum einen bestehen unterschiedliche Risikoneigungen und zum anderen ist Risiko abhängig vom jeweiligen Informationsstand (Kaplan, Garrick 1981, 12).
Trotz der Heterogenität der verschiedenen Sichtweisen weisen diese Gemeinsamkeiten auf. Zum einen liegt den Risikobegriffen der Aspekt der Unsicherheit zugrunde, was bedeutet, dass ein Ereignis eintreten kann oder nicht. Zum anderen sind die unerwünschten Ereignisse, die sich aus einer betriebswirtschaftlichen Sichtweise in Kosten bzw. Verlusten ausdrücken lassen, ein weiteres Element der verschiedenen Risikoauffassungen (DeMarco, Lister 2003, 11; Wallmüller 2004, 6). Zudem liegen dem Risiko unabhängig von der gewählten Definition dem Risikobegriff zukünftige Sollvorstellungen zugrunde, von denen Abweichungen bestehen können (Füser et al. 2002, 496; Wolf 2005, 26).
Sowohl Bitz als auch Schulte zeigen die Zusammenhänge zwischen den verschiedenen Sichtweisen auf Risiko auf, indem sie eine Integration vornehmen. Dieser Arbeit liegt folgendes Risikoverständnis zugrunde:

Risiko wird als die Möglichkeit der Gefahr von Verlusten im Rahmen der Geschäftstätigkeit, d.h. des negativen Abweichens der Unternehmensentwicklung von geplanten Größen bzw. Zielen verstanden, die ursachenbezogen aus der generellen Unsicherheit zukünftiger Ereignisse, verbunden mit einem unvollständigen Informationsstand resultiert (Schulte 1997, 12; Bitz 2000, 13).

Nach der Betrachtung der verschiedenen Strömungen innerhalb des betriebswirtschaftlichen Risikoverständnisses, werden nachfolgend unterschiedliche Risikotypen, die als dichotome Paare spezifiziert werden können, erläutert.

3.2 Risikotypen

Neben unterschiedlichen Perspektiven auf den Risikobegriff werden nachfolgend verschiedene Risikotypen erläutert, um die Spannbreite des Konzeptes Risiko aufzuzeigen. Die unterschiedlichen Typen sind dabei insbesondere für die Steuerung von Relevanz (siehe 3.5). Dabei werden im Folgenden (1) reine vs. spekulative, (2) interne vs. externe, (3) Aktions- vs. Bedingungs-, (4) versicherbare vs. nicht versicherbare, (5) regulatorisch zu steuernde vs. optionale sowie (6) operative vs. strategische Risiken voneinander abgegrenzt[72].

(1) reine vs. spekulative Risiken: Reine Risiken gehen auf die Versicherungswirtschaft zurück und spiegeln das anglo-amerikanische Risikoverständnis wider. Sie führen nur zu Verlusten und schließen positive Abweichungen bzw. Chancen aus der Betrachtung aus (Farny 1979, 20f; Lück et al. 2002, 230; Altenburger 2003, 150). Im Gegensatz dazu sind spekulative Risiken mit unsicheren Ereignissen verbunden, die sich durch das unternehmerische Handeln vermögensmindernd oder -mehrend auswirken können (von Werder 1992, 2212; Altenburger 2003, 150; Schomann, Bloech 2005, 225). Nach einer weiten Auffassung, bei der auch Chancen eingeschlossen werden, werden spekulative Risiken zugrunde gelegt.

(2) interne vs. externe Risiken: Legt man den Einflussbereich des Unternehmens bei der Klassifikation zugrunde, so kann im Hinblick auf die Herkunft in externe bzw. außerbetriebliche und interne bzw. innerbetriebliche Risiken unterschieden werden (Mikus 2001, 8; Schorcht 2004, 26). Externe Risiken unterscheiden sich in ihrer Beeinflussbarkeit durch das Unternehmen. So können externe Risiken aus dem natürlichen (z.B. Naturereignisse), dem globalen (z.B. Regulation) etc. oder sozialen Umfeld (z.B. Standort) entstammen. Letztendlich können Risiken auch unternehmensintern verursacht werden. Die Beeinflussbarkeit der Risiken nimmt dabei in der Reihenfolge der Nennung zu (Schorcht 2004, 103ff). Somit können primär interne Risiken durch eigene Handlungen beeinflusst werden (z.B. Investitionen, Reorganisationen). Zudem existieren vielfach hybride Risiken, die sich aus dem Zusammenwirken interner und externer Faktoren ergeben (Aubert et al. 2002, 157f).

(3) Aktions- vs. Bedingungsrisiken: Weiterhin kann eine Unterscheidung in Aktions- und Bedingungsrisiken vorgenommen werden (Haller 1978, 485). Aktionsrisiken haben zum Gegenstand, dass durch getroffene Entscheidungen oder aufgrund der Durchführung ungeeigneter Maßnahmen die gesetzten Unternehmensziele nicht erreicht werden. Sie erwachsen somit aus Handlungen des Unternehmens. Bedingungsrisiken hingegen betreffen die meist unbewusst vorausgesetzten Randbedingun-

[72] Quellen für verschiedene Typen sind: (Mikus 2001, 7ff; Altenburger 2003, 150; Schorcht 2004, 24ff).

gen der Geschäftstätigkeit und sind nicht auf Handlungen des Unternehmens zurückzuführen, sondern gefährden die Zielerreichung durch unerwartete Änderungen der Rahmenbedingungen (Haller 1978, 485).

(4) versicherbare vs. nicht versicherbare Risiken: Als weitere Typisierung kann zwischen Risiken, die theoretisch versicherbar bzw. nicht versicherbar sind unterschieden werden. Erstgenannte Kategorie schließt Risiken ein, die unabhängig davon, ob ein Versicherungsangebot existiert oder nicht versicherbar wären. Nicht versicherbare Risiken schließen v.a. das allgemeine Unternehmerrisiko ein, das nicht kalkulierbar ist und auch aus der Kostenrechnung ausgeklammert wird (Altenburger 2003, 150).

(5) regulatorisch zu steuernde vs. optionale Risiken: Risiken können im Hinblick auf die Regulation unterschieden werden (Williams et al. 2006, 69). So sind beispielsweise bestandsgefährdende Risiken nach KonTraG oder Betrugs- und Diebstahlsrisiken nach Basel II zu steuern (siehe 3.6). Darüber hinaus bestehen Risiken, für die keine explizite Regulation besteht. Sie werden daher auch als optionale Risiken bezeichnet. Dabei liegt der Umgang mit diesen Risiken im Ermessen des jeweiligen Unternehmens und ist abhängig von der individuellen Risikobereitschaft (Williams et al. 2006, 69). Je nach Ausmaß der Regulation, die über Branchen hinweg variiert, ist der Anteil der optionalen Risiken unterschiedlich hoch.

(6) operative vs. strategische Risiken: Risiken können entsprechend ihres strategischen Gehalts in operative und strategische Risiken unterschieden werden (Wyss 2000, 179; Romeike 2004a, 41). Diese Unterscheidung geht dabei auf die beiden Handlungsebenen operatives und das strategische Management zurück. Während sich operatives Management mit der unmittelbaren eher kurzfristigen Steuerung des unternehmerischen Wertschöpfungsprozesses befasst, abstrahiert das strategische Management davon und ist auf die Bearbeitung langfristiger Aufgaben angelegt (Ulrich, Fluri 1995, 18ff; 114). Somit sind strategische Risiken durch einen gewissen Grundsatzcharakter gekennzeichnet und können als komplexe Problemsituation beschrieben werden, die durch vielfältige Einfluss- und Handlungsfaktoren, einen langfristigen Wirkungshorizont und einem hohen Grad an informatorischer Unvollkommenheit gekennzeichnet sind. Operative Risiken hingegen beschreiben eine vergleichsweise einfacher durchschaubare Problemsituation, sind stärker einzelfallbezogen, wirken eher kurzfristig, weisen einen höheren Detaillierungsgrad auf, sind durch einen geringeren Grad an informatorischer Unvollkommenheit gekennzeichnet und ergeben sich aus den täglichen betrieblichen Tätigkeiten (Hermann 1996, 29; Schulte 1997, 19ff; Wyss 2000, 179). Umso mehr die Risiken durch strategische Unsicherheiten charakterisiert sind, desto schwieriger sind sie zu adressieren. Aufgrund ihrer Komplexität sind strategische Risiken zum Teil nicht oder nur schwer quantifizierbar und werden vorzugsweise anhand qualitativer Aspekte bewertet und gesteuert (Helmke, Risse 1999, 277; Pfitzer et al. 2002, 2005; Norrman, Lindroth 2004, 20).

Von den dargestellten Typisierungen sind alle genannten Risikotypen für die nachfolgenden Betrachtungen von Relevanz. So werden sowohl reine als auch spekulative Risiken betrachtet, wobei primär reine Risiken fokussiert werden und eine negative Begriffsauffassung zu Risiko zugrunde gelegt wird. Ebenso sind interne und externe sowie Aktions- und Bedingungsrisiken Gegenstand der nachfolgenden Risikobetrachtungen. Der Aspekt der Versicherbarkeit ist insbesondere bei der Analyse der Steuerbarkeit von Risiken bedeutend, die im Kontext des RM von Relevanz ist (siehe 3.5). Der Aspekt der Regulation wird durch eine gesonderte Betrachtung in Abschnitt 3.6 gewürdigt. Im Falle der Unterscheidung zwischen operativen und strategischen Risiken erfolgt eine Fokussierung auf erstgenannte, da diese Risiken auf der Ebene der Geschäftsprozesse verortet sind und wie zuvor dargestellt, im Hinblick auf die Identifizier-, Bewert- und Steuerbarkeit Vorzüge aufweisen. Darüber hinaus sind für Unternehmen insbesondere Risiken von Relevanz, die sich aus dem täglichen Umgang bzw. dem Einsatz von Ressourcen ergeben. Aufgrund ihrer Charakteristika, die mit dem Untersuchungsgegenstand dieser Arbeit korrespondieren, werden im folgenden Abschnitt operationelle Risiken detailliert betrachtet.

3.3 Operationelles Risiko

Die Bedeutung der in Abschnitt 3.2 thematisierten Unterscheidung zwischen strategischen und operativen Risiken zeigt sich v.a. auch in der verstärkten Betrachtung von Risiken auf der Ebene der operativen Geschäftsprozesse. Bei Banken wird dieser Risikotyp als operationelles Risiko bezeichnet, wobei diese Risiken per se nicht bankspezifisch sind, sondern auch allgemein betriebswirtschaftlich als Betriebsrisiken bezeichnet werden. Es handelt sich dabei auch nicht um eine vollkommen neue Risikokategorie, da diese Risiken mit der Geschäftstätigkeit bzw. Leistungserstellung einhergehen (Klomfass, Quadt 2001, 322f; Einhaus 2002, 488). Somit ist die Existenz operationeller bzw. Betriebsrisiken bedingt durch ihren engen Bezug zur Geschäftstätigkeit seit langem bekannt. Jedoch erfolgte in Unternehmen in der Vergangenheit nur selten eine gezielte bzw. systematische Auseinandersetzung und vielfach eine Unterschätzung dieser Risiken (Wyss 2000, 179; Jovic, Piaz 2001, 923f). Das in den letzten Jahren gestiegene Interesse an dieser Thematik ist dabei allgemein auf die Zunahme operationeller Risiken und insbesondere auf prominente Unternehmenskrisen, vermehrte Regulation durch Gesetzgeber oder spezifische Institutionen sowie das Streben nach einer ganzheitlichen Risikobetrachtung zurückzuführen (Geiger, Piaz 2001, 790; Foit 2005, 20). Motiviert durch diese Faktoren erfolgte seit 1999 eine intensive Auseinandersetzung mit operationellen Risiken bei Banken. Diese geht soweit, dass durch den Baseler Ausschuss für Bankaufsicht im Rahmen der Einführung von Basel II ein systematisches Management operationeller Risiken ebenso wie eine Eigenkapitalhinterlegung dieser Risiken gefordert wird. Nach dem Baseler Ausschuss für Bankaufsicht wird operationelles Risiko wie folgt definiert:

Operationelles Risiko bezeichnet die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten (Basel 2004, 157)[73].

In dieser Definition sind Rechtsrisiken eingeschlossen und strategische sowie reputationsbezogene Risiken ausgeschlossen. Der Begriff geht ursprünglich auf die British Bankers Association zurück, die im Wortlaut gleich war, jedoch eine Unterscheidung in mittelbare und unmittelbare Verluste vornahm, wobei letztere z.B. Opportunitätsverluste durch das Auslassen von Chancen einschloss. Dieser Unterteilung wurde bis 2001 auch noch durch den Baseler Ausschuss gefolgt, jedoch dann verworfen, da bedingt durch die Einforderung einer Eigenkapitalhinterlegung das Auslassen von Chancen zu Bestrafungen geführt hätte und nur Risiken im engeren Sinne hinterlegt werden sollten (Füser et al. 2002, 496).

Bezüglich der in Abschnitt 3.1 thematisierten Ursachen- bzw. Wirkungskomponente stellt der operationelle Risikobegriff vorwiegend auf die verschiedenen Ursachen ab, die ihrerseits wiederum zu Verlusten führen (Kuhn 2002, 156). Zudem liegt der Fokus vorwiegend auf internen Risikoursachen, die sich aus Handeln bzw. Unterlassen ergeben. Im Bereich der Banken ist dies ein klares Unterscheidungskriterium zu eher extern fokussierten Markt- und Kreditrisiken (Geiger, Piaz 2001, 792). Die Risikokategorie externe Ereignisse umfasst beispielsweise Naturkatastrophen, Brände, externe Betrugsfälle oder Risken aus Regulation, während Risiken im Bereich der Systeme die Datenqualität, IT-Sicherheitslücken, IT-Ausfallrisiken oder Kompatibilitätsprobleme betreffen. Risiken in Bezug auf die Kategorie Prozesse betreffen z.B. Transaktions-, Rechnungslegungsfehler oder fehlerhafte Gestaltung des Zugangs oder Zugriffs, während Risiken der Kategorie Personen Betrug, mangelnde Kenntnisse, Krankheit etc. einschließen (Piaz 2002, 57; Jorion 2003, 538; KPMG 2003, 3). Verschiedene Autoren führen zusätzlich Organisation als fünfte Ursachenkategorie ein und begrenzen Risiken im Bereich Prozesse auf Schwachstellen in Verfahren, während die Kategorie Organisation verschiedenste Risiken in Bezug auf die organisatorische Verankerung, Projekt- oder Changemanagement umfasst (Doering 2001, 20f; Wallmüller 2004, 22). Da die IT in vielen Unternehmen die Geschäftsprozesse determiniert, sind Risiken bezüglich der IT und im Speziellen der IT-Sicherheit (siehe auch Abschnitt 4.1) aus Sicht der operationellen Risiken eine der bedeutendsten Risikogruppen (Hirschmann, Romeike 2004, 13). IT-Risiken werden vorwiegend der Kategorie Systeme zugeordnet. Da der IT-Einsatz und dessen Sicherheit auch Personen, Prozesse und externe Ereignisse betrifft, kann man allerdings auch die Sichtweise vertreten, dass IT-Risiken einen gewissen Anteil an allen genannten Kategorien haben (Wolf 2005, 56).

[73] Weitere Definitionen zu operationellen Risiken (aus der Sicht von Banken) sind bei Piaz (2002, 58f) zu finden.

Obwohl der operationelle Risikobegriff auf die operative Ebene ausgerichtet ist, sind die Begriffe operationelles und operatives Risiko nicht gleichzusetzen. Operatives Risiko stellt nach angloamerikanischer Auffassung den unternehmensinternen Teil der operationellen Risikosichtweise dar und blendet somit extern verursachte Risiken aus (Piaz 2002, 56). In diesem Kontext sollen jedoch auch extern verursachte Risiken betrachtet werden, weshalb die weitere Sichtweise des operationellen Risikos zugrunde gelegt wird.

3.4 Kategorisierung von Risiken

Nach der Betrachtung unterschiedlicher Perspektiven und Risikotypen wird in diesem Abschnitt eine allgemeine Kategorisierung von Risiken sowie im Speziellen eine Kategorisierung von operationellen Risiken dargelegt, um aufzuzeigen, welche Risiken im Unternehmenskontext betrachtet werden.
In der Literatur besteht eine Vielzahl an Kategorisierungsansätzen, wobei durch individuelle Besonderheiten und unterschiedliche Aktivitäten von Unternehmen, die Entwicklung einer vollständigen bzw. allgemeingültigen Kategorisierung erschwert wird. Diederichs et al. erarbeiten allerdings trotzdem eine derartige Kategorisierung (siehe Abb. 10) und unterteilen in externe, leistungswirtschaftliche, finanzwirtschaftliche Risiken sowie in Risiken aus Management und Organisation (Diederichs et al. 2004, 190)[74]. Unter leistungswirtschaftlichen Risiken werden Risiken aus den Bereichen Beschaffung (z.B. Lieferantenabhängigkeit), Produktion (z.B. geringe Auslastung), Logistik (z.B. zu geringe Transportkapazität), Absatz (z.B. ineffiziente Vertriebsstruktur) und Marketing (z.B. ungenaue Zielgruppenbestimmung) subsumiert (Oehler, Unser 2002, 14; Diederichs et al. 2004, 190). Der Arbeitskreis "Externe und Interne Überwachung der Unternehmung" nennt die Kategorie leistungswirtschaftliche Risiken nicht explizit, sondern sieht Absatz- und Beschaffungsrisiken auf der obersten Ebene (Arbeitskreis 2000, 1ff). Unter finanzwirtschaftlichen Risiken werden Risiken in Zusammenhang mit Kapitalbeschaffung (z.B. schlechtes Rating), Kapitalanlagen (z.B. Renditeunsicherheit), Liquidität (z.B. Forderungsausfall), Währungen (z.B. schwankende Wechselkurse) und Zinsen (z.B. unsichere Zinserträge) zusammengefasst (Diederichs et al. 2004, 190). Als alternative Unterteilung kann bei einem stärkeren finanzwirtschaftlichen Fokus auch in Markt-, Kredit- und Liquiditätsrisiken unterschieden werden (Oehler, Unser 2002, 14). Risiken aus Management und Organisation werden zum Teil als Risiken aus Corporate Governance bezeichnet. Sie umfassen die Bereiche Management (z.B. mangelnde Managementqualität), Organisationsstruktur (z.B. mangelnde Verantwortlichkeiten), Personal (z.B. Fehlverhalten oder Mitarbeiterunzufriedenheit), Forschung und Entwicklung (z.B. Techno-

[74] Ähnliche Kategorisierungen werden durch weitere Autoren wie z.B. (Keitsch 2000, 11; Hiles, Barnes 2001, 31f; Lück et al. 2002, 231; Pfitzer et al. 2002, 2006) vorgenommen, wobei an dieser Stelle die Kategorisierung von Diederichs et al. als Referenzmodell herangezogen wird (siehe Abb. 10), da sie auf einem Gremium basiert, das zum Ziel hat, einen Standard zum RM zu entwickeln (Diederichs et al. 2004, 190). Bedeutende Unterschiede anderer Kategorisierungen werden bei der nachfolgenden Erörterung der Referenzkategorisierung (siehe Abb. 10) einbezogen.

logieabhängigkeit), Informationstechnologie (z.B. IT-Sicherheit, Systemausfälle) und Recht (z.B. Ansprüche aus Produkthaftung) (Gleißner 2001, 119; Pfitzer et al. 2002, 2006; Diederichs et al. 2004, 190). Externe Risiken können in Markt- und Kundenrisiken (z.B. schwache Konjunktur oder Bedrohungen durch Wettbewerber), Politik und Gesetzgebung (z.B. allgemeine Änderungen der Gesetzgebung oder der Subventionierung), natürliche Umwelt (z.B. Naturkatastrophen) oder soziokulturelle Risiken (z.B. gesellschaftliche Veränderungen oder Diebstahl) unterschieden werden (Diederichs et al. 2004, 190). Bei der Kategorisierung von Risiken ist es allerdings schwer, die vorherrschende Risikolandschaft allgemeingültig und überschneidungsfrei zu kategorisieren, da unternehmensindividuell Risiken verbleiben, die unter Umständen keiner Kategorie zugewiesen werden können (Jovic, Piaz 2001, 924).

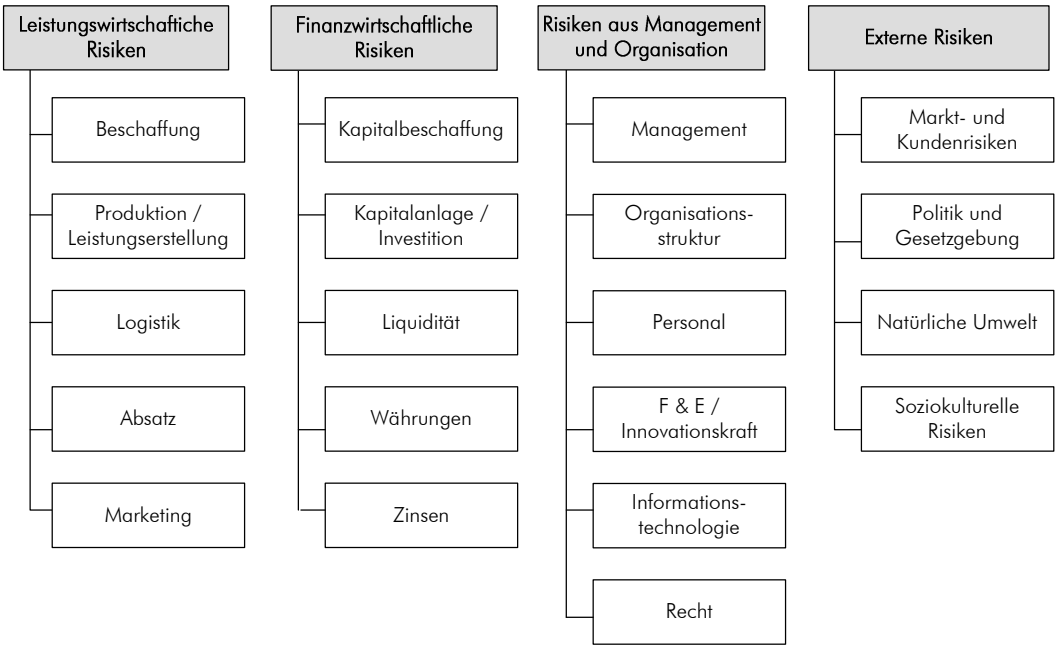


Abb. 10 Risikofelder und Risikoarten[75]

Daher ist diese Kategorisierung auch nicht als statisch zu verstehen, sondern kann um Risikokategorien reduziert bzw. erweitert werden (Diederichs et al. 2004, 190). Insbesondere branchenspezifische Besonderheiten führen zu Variationen und haben zur Folge, dass eine derart generische Kategorisierung nicht immer vollständig ist. Dem trägt der Arbeitskreis "Externe und Interne Überwachung der Unternehmung" Rechnung, indem Branchenrisiken als eigene Risikokategorie definiert werden (Arbeitskreis 2000, 1ff)[76].

[75] Nach (Diederichs et al. 2004, 190).

[76] Einige Autoren betonen, dass es sich bei strategischen Risiken um eine eigene Risikokategorie handelt, die beispielsweise Risiken im Zusammenhang mit der Unternehmensstrategie selbst oder mit Bedrohungen kritischer Erfolgsfaktoren einschließt (Gleißner 2001, 115; Hiles, Barnes 2001, 31).

Im Bankwesen, das sich traditionell mit RM befasst, wird eine Unterteilung in die drei Kategorien Markt-, Kredit- und operationelle Risiken vorgenommen, die im Kontext der Regulation nach Basel II mit einer Eigenkapitalhinterlegung verbundenen sind. Unter Marktrisiken werden Risiken subsumiert, die bei ungünstiger Preisentwicklung zu Verlusten aus bilanzwirksamen und außerbilanziellen Positionen führen. Diese Kategorie schließt beispielsweise Aktienkurs-, Zinsänderungs-, Wechselkurs-, Edelmetallpreis- oder das Rohwarenpreisrisiko ein (Piaz 2002, 16).

Kreditrisiko bezeichnet allgemein das Risiko, dass ein Kreditnehmer seinen Pflichten gegenüber dem Gläubiger nicht mehr nachkommen kann und daraus Verluste entstehen. Ist der Gläubiger ein Kreditinstitut so spricht man auch von einem Adressenausfallrisiko. Das Kreditrisiko wird mit Hilfe von Kennzahlen, so genannten Kredit-Ratings, gemessen, mittels derer die Wahrscheinlichkeit eines Ausfalls beschrieben wird. Das Rating kann entweder extern von einer Ratingagentur (z.B. Standard & Poor's, Moody's und Fitch Ratings) oder auch intern durch IRB-Ansätze[77] durch die Bank selbst vorgenommen werden, wobei nach einer OECD Studie die meisten europäischen Länder auf externe Ratingagenturen zurückgreifen. Ein internes Rating bedarf der Zustimmung der Bankenaufsicht (Basel 2004, 26ff, 54ff; Blommestein 2005, 31). Ein schlechteres Rating wird mittels Risikoprämien auf den Kreditnehmer umgelegt.

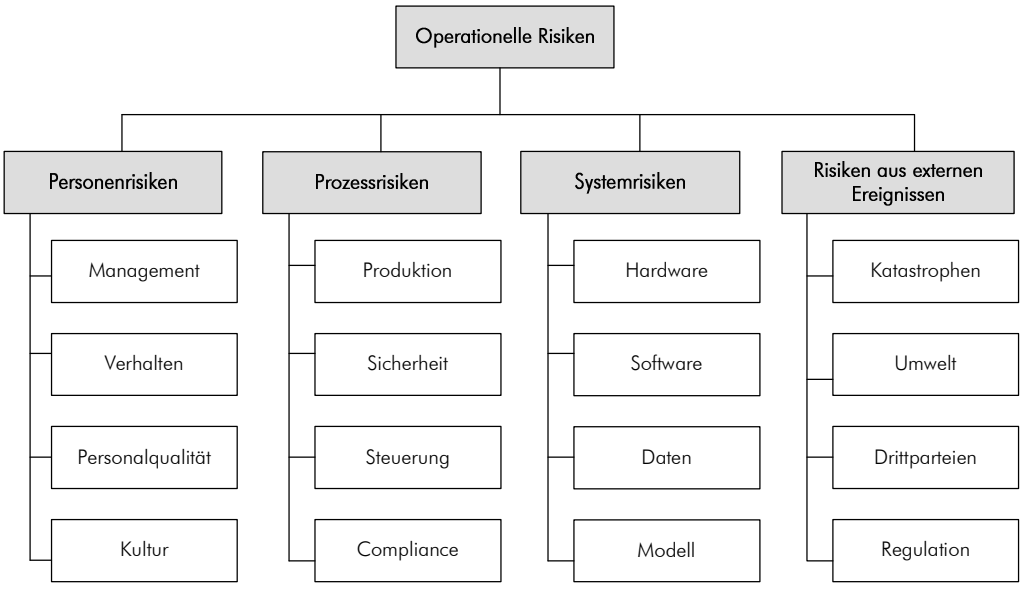


Abb. 11 Kategorisierung operationeller Risiken[78]

Operationelle Risiken als dritte Risikogruppe, die für den Untersuchungsgegenstand aufgrund ihrer Charakteristika von Relevanz sind, weisen nach dem Baseler Ausschuss für Bankaufsicht Prozesse, Personen, Systeme und externe Ereignisse als Risikoursachen auf[79].

[77] Die Abkürzung IRB bedeutet Internal Rating Based.
[78] In Anlehnung an (Piaz 2002, 57).
[79] Siehe hierzu Abschnitt 3.3.

Zur Detaillierung wird die Unterteilung von Piaz herangezogen, da sie unter dem Versuch der Bildung von Oberkategorien die wesentlichen Aspekte abdeckt und in Anlehnung an den operationellen Risikobegriff eine Unterteilung in Personen-, Prozess-, Systemrisiken und Risiken aus externen Ereignissen vornimmt (siehe Abb. 11) (Piaz 2002, 57)[80]. Nach dieser Kategorisierung (siehe Abb. 11) können Personenrisiken in die Bereiche Management (z.B. Führungs- und Durchsetzungsrisiken), Verhalten (z.B. Betrug oder Irrtum), Personalqualität (z.B. mangelnde Fähigkeiten oder Fertigkeiten) oder Kultur (z.B. hohe Fluktuation oder Kommunikationsbarrieren) unterteilt werden (Kuhn 2002, 157; Piaz 2002, 57). Unter Prozessrisiken werden Risiken der Produktion (z.B. Transaktionsrisiken), Sicherheit (z.B. Zutrittsrisiken), Steuerung (z.B. fehlerhaftes Reporting oder Monitoring) oder Compliance (z.B. Dokumentationsrisiken) subsumiert. Hardware (z.B. Ausfall von Systemen), Software (z.B. mangelnde Kompatibilität), Daten (z.B. mangelnde Datenqualität) und Modell (z.B. Fehler in Modellen und Anwendungen) stellen Unterkategorien für Risiken der Kategorie System dar (Piaz 2002, 57). Risiken aus externen Ereignissen können unterschiedliche Ursprünge haben und in den Kategorien Katastrophen (z.B. Naturgewalten), Umwelt (z.B. Altlastenentsorgung), Drittparteien (z.B. externer Betrug) oder Regulation (z.B. Steueränderungen) auftreten (Piaz 2002, 57). Jorion betont, dass externe Risiken zum Teil eine physische Komponente aufweisen. So wirken sich Risiken im Zusammenhang mit Feuer, Naturkatastrophen, physische Sicherheit, Terrorismus und Diebstahl physisch aus (Jorion 2003, 538). Neben externen Risiken nimmt Kuhn eine abweichende und feinere Unterteilung von Risken ohne physische Komponente in politische, gesetzliche und rechtliche Risiken. Erstere beinhalten z.B. soziokulturelle und marktliche Veränderungen, während sich die beiden letztgenannten Kategorien aus Gesetzgebung und Rechtsprechung bzw. deren Änderung ergeben (Kuhn 2002, 157). Mögliche Drittparteien sind z.B. Kunden, Lieferanten oder Partner (Seibold 2006, 17).

Vergleicht man die beiden Kategorisierungen (siehe Abb. 10 und Abb. 11), so ergeben sich starke Schnittmengen und es zeigt sich, dass operationelle Risiken auch Bestandteil der allgemeinen branchenunabhängigen Kategorisierung sind. So korrespondieren die Kategorien externe Ereignisse nach Basel II mit den externen Risiken, während sich die übrigen Ursachen vorwiegend in der Kategorie Management und Organisation niederschlagen. Die Kategorie Prozesse aus dem Modell operationeller Risiken findet sich in den Unterkategorien Management und Organisationsstruktur, während Personen und Personal korrespondieren. Die Kategorie Informationstechnologie entspricht der Risikoursachenkategorie Systeme.

Ebenso wie bei Risiken im Allgemeinen besteht auch bei operationellen Risiken das Problem, dass es oftmals schwer fällt, Risiken eindeutig einer Kategorie zuzuordnen, da mehrere Kategorien betroffen sein können. Eine Zuordnung fällt v.a. dann einfacher, wenn die Risiken schon einmal aufgetreten

[80] Ebenso wie bei Risiken im Allgemeinen wird bei der Betrachtung operationeller Risiken in der Literatur eine unterschiedliche Kategorisierung bzw. Spezifizierung verfolgt (Doering 2001, 20; van den Brink 2001, 4ff; Piaz 2002, 57; Simon 2002, 130ff; Stickelmann 2002, 12; Jorion 2003, 538; KPMG 2003, 3).

sind und die Ursachen und Wirkungen bekannt sind (Stickelmann 2002, 13). Insbesondere die Trennschärfe zwischen der Kategorie Personen und den anderen Ursachenkategorien ist zum Teil schwer erreichbar, da Personen vielfach beteiligt sind, da sie z.B. Aktivitäten in Prozessen ausführen. Um Trennschärfe zur gewährleisten, wird bei der Kategorisierung von Risiken von einer primären Ursachenzuordnung ausgegangen. Anhand eines Beispiels bedeutet dies, dass der Kategorie Personen nur diejenigen Risiken zugeordnet werden, die direkt z.B. durch menschliches Versagen oder kriminelle Handlungen verursacht werden (Seibold 2006, 16). Insgesamt haben derartige Klassifizierungen zum Vorteil, dass sie die Identifikation von Risiken unterstützen bzw. zu deren Strukturierung beitragen. Dabei ist es besonders werthaltig, wenn Standards bestehen, die in verschiedenen Unternehmen erprobt wurden und sich bewährt haben, da sie Best Practices zur Risikoidentifikation darstellen.

3.5 Kern- und Unterstützungsaufgaben im Risikomanagement

Eine gezielte Auseinandersetzung mit Risiken in Unternehmen ist auf eine Reihe von unternehmensextern und -intern veranlassten Motivationsfaktoren zurückzuführen, wobei erstere die verschiedenen Regulationen (siehe 3.6) betreffen. Unter die internen Motivationsfaktoren sind die Aufrechterhaltung der Geschäftstätigkeit sowie die Gewährleistung der Wirtschaftlichkeit zu subsumieren (Jonen, Müller 2006, 143f). Darüber hinaus kann unterstellt werden, dass jedes Unternehmen nach einem Mindestmaß an Sicherheit bzw. nach einer Begrenzung der Risikolage strebt und dessen Erreichung das Ergreifen von Maßnahmen erforderlich macht (Farny 1979, 18f).

Ebenso wie der Risikobegriff, kann auch der RM-Begriff unterschiedlich weit gefasst werden. Die Disziplin RM hat sich in den frühen 50'er Jahren aus der Praxis amerikanischer Industriebtriebe entwickelt, in denen das Berufsbild des Versicherungsexperten zum Risikomanager ausgedehnt wurde[81]. In der wissenschaftlichen Literatur wurde durch Mehr und Hedges (1974) ein Ansatz entwickelt, der die Optimierung des betrieblichen Versicherungsschutzes zum Gegenstand hatte und Risikoaspekte einschloss. Seit den 70`er Jahren wird RM auch im deutschen Sprachraum thematisiert. Nach diesem klassischen Verständnis befasst sich RM mit der Frage, inwiefern Risiken durch Versicherungen abgedeckt werden können und sollen (von Werder 1992, 2212; Karten 1993, 3826; Merbecks 1995, 25; Simister 2000, 9). Dabei ist der versicherungswirtschaftliche Aspekt nur ein Teil des RM, der sich damit befasst, durch die Zahlung einer Prämie die Eintrittswahrscheinlichkeiten von Risiken zu verändern bzw. das Risiko zu überwälzen. Somit ist der Gegenstand in diesem Fall die Schadensversicherung (Ritchie, Marshall 1993, 13).

RM geht allerdings weit über versicherungswirtschaftliche Fragestellungen hinaus und kann neben dieser engen Auslegung RM auch weit gefasst und als Teil der Unternehmensführung angesehen wer-

[81] In den 70'er Jahren erweiterte die Association of Insurance Managers in Industry and Commerce (AIMIC) ihre Bezeichnung auf Association of Insurance and Risk Managers in Industry and Commerce (AIRMIC) (siehe auch http://www.airmic.com).

den (von Werder 1992, 2212; Wall 2001, 212; Archbold 2005, 31)[82]. In diesem Kontext wird der weitere Begriff zugrunde gelegt und RM als die Gesamtheit aller organisatorischen Regelungen und Maßnahmen zur Identifikation, Bewertung, Steuerung und Überwachung von Risiken gesehen (Farny 1979, 19; Schulte 1997, 13; IDW 1999, Tz 4; Erdenberger 2001, 14; Wallmüller 2004, 10). Durch den systematischen Umgang mit Risiken sollen potentielle Verluste auf ein akzeptables Ausmaß reduziert werden und so die Überlebensfähigkeit des Unternehmens gewährleistet werden. Schulte betont, dass RM Maßnahmen zur planmäßigen und zielgerichteten Analyse Steuerung und Kontrolle der Risikoposition umfasst, wobei planmäßig in diesem Zusammenhang bedeutet, dass die Maßnahmen systematisch und dauerhaft getroffen werden, während sich der Begriff zielgerichtet auf einen Soll-Ist Vergleich bezieht (Schulte 1997, 13). Dabei schließt RM auch die Definition von Kennzahlen zur Quantifizierung finanzieller Verlust, die durch unerwartete oder zufällige Veränderungen oder Ereignisse verursacht werden, ein (Gorrod 2004, 3).

Insgesamt besteht das primäre Ziel des RM darin, Risiken so früh wie möglich zu identifizieren, zu beurteilen, zu steuern und permanent zu überwachen, um die langfristige Anpassung des Unternehmens an die Dynamik der Umfeldbedingungen und somit die Erreichung der Unternehmensziele, die nachhaltige Erhöhung des Unternehmenswertes sowie letztlich den Unternehmensfortbestand sicherzustellen. Darüber hinaus ist auch die Optimierung der Risikokosten ein bedeutendes ökonomisches Ziel (Romeike 2002, 14; Reichmann, Form 2003, 169). Aus strategischer Sicht besteht das Ziel des RM darin, Risikopotentiale, die eine nachhaltig erfolgreiche Unternehmensentwicklung gefährden können, frühzeitig zu erkennen und durch geeignete proaktive oder reaktive Maßnahmen zu bewältigen, wobei zur Erreichung dieses Ziels Frühwarnindikatoren eingesetzt werden können (Oepping, Siemes 2003, 229ff).

Neben der Steuerung erfolgsgefährdender Risiken, ist nach einem weiten Verständnis auch die Identifikation von Chancen mit ihren entsprechenden Erträgen einzuschließen (Hornung et al. 1999, 318). Hinsichtlich einer chancenfokussierten Betrachtung stellt RM auch die Quelle von Wettbewerbsvorteilen dar, die sich aus einer vergleichsweise besseren Steuerung der Risiken ergeben und sich positiv auf die Gewinne und das Wachstum des Unternehmens auswirken können (Kimball 2000, 5; Kubitscheck 2000, 38). Dabei ist allerdings nicht nur die Vermeidung potentieller Risiken, sondern auch die Schaffung von Handlungsspielräumen, die ein bewusstes Eingehen von Risiken ermöglichen, Gegenstand des RM (Wallmüller 2004, 4). Somit ist das Ziel des RM nicht in der Eliminierung sämtlicher Risiken zu sehen, sondern vielmehr in deren Reduktion auf ein akzeptables Maß, das sich aus der Risikoneigung sowie dem Verhältnis zwischen Schadensausmaß und Aufwand der zu ergreifenden

[82] Hinsichtlich der Entwicklung des RM betonen Spira und Page, dass Risiko nach einem frühen Verständnis als Schicksal aufgefasst wurde, nach der aktuellen Sichtweise als kalkulierbar bzw. quantifizierbar und zukünftig im Zuge der intensiveren Auseinandersetzung mit dieser Disziplin als kontrollierbar gesehen wird (Spira, Page 2003, 645).

Maßnahmen ergibt (Erdenberger 2001, 13; Peltier 2001, 2; Strulik 2001, 41). Nach einem prozessorientierten Verständnis wird RM vielfach auch als kontinuierlicher Prozess aufgefasst, der die Kernaufgaben[83] Identifikation, Bewertung, Steuerung und Überwachung der Risiken umfasst, direkt von den Veränderungen des internen und externen Umfeldes abhängt und zur Reduktion der Eintrittswahrscheinlichkeit bzw. des Schadensausmaßes der Risiken dient (Tchankova 2002, 290; Norrman, Lindroth 2004, 22; Wallmüller 2004, 10; Archbold 2005, 31; Williams et al. 2006, 67). Diesen Kernaufgaben wird durch die Risikostrategie eine Ausrichtung vorgegeben, die mit den Unternehmenszielen korrespondiert, während die Risikokommunikation und -dokumentation unterstützende Aufgaben darstellen (siehe Abb. 12). In den folgenden Abschnitten werden die Kern- und Unterstützungsaufgaben dargestellt, wobei zunächst die Risikostrategie erörtert wird, da durch sie eine Gesamtausrichtung des RM vorgegeben wird.

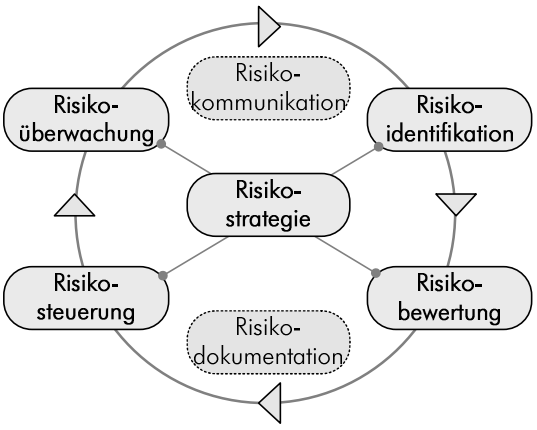


Abb. 12 Kernaufgaben des RM-Prozesses

3.5.1 Risikostrategie

Die Risikostrategie umfasst die Formulierung der Zielstellungen des RM und gibt so die Ausrichtung des Prozesses vor (Bitz 2000, 25; Erdenberger 2001, 14; Altenburger 2003, 151; Junginger et al. 2003, 358; Locher et al. 2004, 25; Wolf 2004, 14). Aufgrund der unmittelbaren Verantwortung durch das Management und der Ableitung der RM-Ziele aus den Unternehmenszielen nimmt die Risikostrategie eine übergeordnete Stellung ein (Erdenberger 2001, 14; Kuhn 2002, 158). Neben der Formulierung der Ziele ist auch die grundlegende Organisation und Verankerung des RM im Rahmen der Risikostrategie festzulegen (Romeike 2002, 14).

In diesem Zusammenhang ist es entscheidend, dass die mit der RM-Strategie verbundene Absichtserklärung verbindlich durch die Unternehmensleitung kommuniziert wird (Romeike 2002, 14). Im Rahmen der Risikostrategie sind Fragestellungen zur Risikotragfähigkeit und Risikobereitschaft zu erörtern (Locher et al. 2004, 25). Dabei wird festlegt, welches Verhältnis zwischen Chancen und Risiken in den einzelnen Geschäftsbereichen einzuhalten ist und ab welcher Schadenshöhe Maßnahmen zur Risikobewältigung eingeleitet werden müssen (Bitz 2000, 19). Ferner stellt bezüglich Tragfähigkeit nicht jeder Verlust zugleich ein Risiko dar, sondern das Risiko ist vielmehr in den unerwarteten Verlusten, die über geplante Verluste hinausgehen, zu sehen. Somit ergibt sich das Risiko aus uner-

[83] Dabei besteht in der betriebswirtschaftlichen Literatur weitgehend Einigkeit über diese Kernaufgaben (Farny 1979, 31; Gleißner, Meier 2001, 55ff; Pfitzer et al. 2002, 2006; Romeike 2002, 14; Reichmann, Form 2003, 171f).

warteten Abweichungen. Zudem kann in Abhängigkeit der finanziellen Lage des Unternehmens eine Unterscheidung in akzeptable und inakzeptable Risiken vorgenommen werden, die die Risikotragfähigkeit widerspiegelt (Geiger, Piaz 2001, 791). Der Umgang mit Risiken ist zudem von der Risikobereitschaft, die in die Zustände risikoavers, -neutral und -freudig unterteilt werden kann, abhängig (Piaz 2002, 10). Diese variiert je nach Präferenz des Unternehmens bzw. des jeweiligen Risikoverantwortlichen.

Im Rahmen des Modells zum RM der European Foundation for Quality Management (EFQM) wird neben der Bestimmung der RM-Ziele eine eigene Phase zur Planung hervorgehoben, die detailliert, wie diese Ziele erreicht werden sollen und welche Ressourcen dazu erforderlich sind (EFQM 2005, 17ff; Williams et al. 2006, 72). Wolf betont in diesem Kontext den zeitlichen Bezug und unterscheidet im Rahmen der Risikostrategie zwischen strategischer, also eher langfristiger sowie operativer d.h. eher kurzfristiger Planung, die jeweils eine unterschiedliche Behandlung der Risiken nach sich zieht (Wolf 2004, 214).

Die Risikostrategie ist dabei vom Normen- und Wertegerüst des Unternehmens abhängig, das sich in einer risikoorientierten Unternehmenskultur widerspiegelt und die Basis für den bewussten Umgang Risiken über alle Hierarchieebenen und Funktionsbereiche hinweg schafft (PWC 2001, 19). Auf Basis der Risikostrategie werden nachfolgend die Kernaufgaben des RM erörtert.

3.5.2 Risikoidentifikation

Die Risikoidentifikation dient als Informationsbasis für die nachgelagerten Prozessphasen. Dabei werden die Ziele der Phase, der allgemeine Gegenstand, die potentiellen Ausgangspunkte, organisatorische Verantwortlichkeiten, Instrumente sowie letztendlich Limitationen dargelegt.

Im Rahmen der Risikoidentifikation sollen die potentiellen Risiken, denen Unternehmen ausgesetzt sind, erfasst werden. Dabei erfolgt die Erfassung von Risiken strukturiert und detailliert und hat die Suche nach bestehenden und latent gefährdenden Entwicklungen bzw. Gefahrenereignissen sowie die Aufdeckung daraus resultierender Wirkungen zum Gegenstand (PWC 2001, 19; Romeike 2002, 15; Tchankova 2002, 291; Diederichs et al. 2004, 192). Alternativ kann man bei der Risikoidentifikation auch von den potentiellen Folgen ausgehen und über die Bildung von Szenarien die Ursachen identifizieren (DeMarco, Lister 2003, 126ff). Einige Autoren lagern der Phase Risikoidentifikation die Definition von Risikofeldern vor, deren Bestimmung als Ausgangspunkt für die Risikoidentifikation dient (Bitz 2000, 25; Reh 2001, 34; Pfitzer et al. 2002, 2006). Nach einer zeitlichen Abgrenzung kann die Risikoidentifikation erstmalig als Initialinventur bzw. regelmäßig oder außergewöhnlich erfolgen (Mosiek 2003, 16). Aufgrund der sich laufend ändernden Unternehmenssituation ist die Identifikation von Risiken als eine kontinuierliche Aufgabe zu verstehen (Romeike 2004a, 48).

Die Identifikation kann je nach Unternehmen aus verschiedenen Perspektiven erfolgen und primär Geschäftsfelder, Prozesse oder vordefinierte Risikokategorien nutzen (Hornung et al. 1999, 320; Einhaus 2002, 490; Romeike 2002, 15). Bei einer Risikoidentifikation nach Geschäftsfeldern werden diese regelmäßig und systematisch untersucht und die erfassten Risiken nach Unternehmensbereichen systematisiert (PWC 2001, 19). Bei einem prozessorientierten Vorgehen erfolgt die Identifikation entlang der Kernprozesse bzw. der Primär- und Sekundäraktivitäten der Wertschöpfungskette, wobei insbesondere dem Einbeziehen kritischer Geschäftsprozesse eine besondere Bedeutung zukommt (Hornung et al. 1999, 320; Einhaus 2002, 490; Junginger et al. 2003, 358). Ferner können vordefinierte Risikokategorisierungen (siehe Abb. 10 und Abb. 11) eine systematische Erfassung unterstützen (Happel, Liebewein 2000, 5; Diederichs et al. 2004, 190). Weitere Basisinformationen, die eine Priorisierung der detailliert zu analysierenden Geschäftsfelder oder Prozesse ermöglichen, können aus verschiedensten Quellen, wie z.B. Personalstatistiken, Dokumentationen zu Systemausfällen, Revisionsberichten oder Kundenbeschwerden, gewonnen werden (van den Brink 2001, 20ff).

Im Hinblick auf die organisatorische Verantwortlichkeit können Mitarbeiter aus verschiedenen Managementebenen in die Identifikation einbezogen werden (Tchankova 2002, 290; von Hohnhorst 2002, 101f). Eine Erfassung auf den operativen Ebenen hat zum Vorteil, dass das Risikobewusstsein vergleichsweise höher ist (Simons 1999, 86). Als problematisch erweisen sich v.a. entgegenstehende persönliche Interessen der jeweiligen Risikoverantwortlichen, die sich z.B. daraus ergeben, dass die Angabe eines Risikos mit dem Eingeständnis eines eigenen Fehlers gleich läuft (Wallmüller 2004, 27). Dennoch wird in der Forschung und Praxis überwiegend die Auffassung vertreten, dass insbesondere die dezentrale Erfassung aufgrund der größeren Problemnähe und des dezentral vorhandenen Fachwissens der Risikoverantwortlichen einen positiven Beitrag zur Vollständigkeit und Qualität der Risikoidentifikation leistet (Erdenberger 2001, 15; Peltier 2001, 2; Piaz 2002, 81; Diederichs, Kaminski 2003, 702; Schmitting, Siemes 2004, 105). Zusätzlich können neutrale Fachexperten (z.B. externe Unternehmensberater), die auf den entsprechenden Gebieten über Fachwissen verfügen, einbezogen werden (Gleißner 2001, 255).

Die Risikoidentifikation kann dabei durch verschiedenste Instrumente und Methoden unterstützt werden. Diese reichen von Workshops, standardisierten Interviews, Brainstormings, Checklisten, Prozessanalysen, Analysen von Produktlebenszyklen bis hin zu Fehlerbaumanalysen etc. (Hornung et al. 1999, 320; Mott 2001, 204; Füser et al. 2002, 497; Leidinger 2002, 244; Diederichs et al. 2004, 191; Romeike 2004a, 49f)[84]. Diese Methoden unterscheiden sich im Hinblick auf den mit ihrem Einsatz verbundenen Aufwand bzw. Kosten und ihrer Eignung („Identifikationstauglichkeit“). So sind nach einer Kategorisierung von Füser et al. beispielsweise Simulationsverfahren, Self Assesments, Szena-

[84] Die unterschiedlichen Methoden lassen sich nach Piaz in die Kategorien Kollektions-, Kreativitäts-, analytische Such- und derivative Identifikationsmethoden unterteilen (Piaz 2002, 81ff).

riotechniken oder Fehlerbaumanalysen gegenüber Befragungen oder Checklisten mit einem vergleichsweise hohen Aufwand verbunden und insbesondere auch die Befragung für die Identifikation geeignet (Füser et al. 2002, 497). Gleißner teilt diese Auffassung im Falle einer umfassenden Befragung der Mitarbeiter nicht und betont, dass schriftliche oder mündliche Befragungen sehr arbeitsaufwendig und nicht besonders leistungsfähig sind, da einerseits Risiken doppelt genannt werden und andererseits zwar aktuelle, aber eventuell nicht besonders bedeutende Risiken gesammelt werden (Gleißner 2001, 114). Diese unterschiedlichen Sichtweisen sind ein Indiz dafür, dass die Güte der jeweilig ergriffenen Maßnahmen von den besonderen Gegebenheiten des anwendenden Unternehmens abhängig sind und auch zuvor als eher ungeeignet eingestufte Maßnahmen im konkreten Anwendungsfall vergleichsweise leistungsfähig sein können (Füser et al. 2002, 497f).

Die Vollständigkeit und Qualität der Risikoidentifikation wird durch eine Reihe an limitierenden Faktoren eingeschränkt. So können Probleme darauf zurückgeführt werden, dass der Prozess zur Risikoidentifikation von Personen ausgeführt wird und diese in Abhängigkeit der Umfeldbedingungen Adaptionen vornehmen, spezifische Sachverhalte interpretieren und improvisieren. Dies impliziert eine gewisse Fehleranfälligkeit. Darüber hinaus besteht zum Teil ein hoher Spezialisierungsgrad, der zur Folge hat, dass nur wenige Personen den vollständigen Prozess der Risikoidentifikation sowie dessen Interaktionen mit anderen Personen oder Systemen vollständig verstehen. Durch die Fluktuation dieser Schlüsselmitarbeiter kann wichtiges Wissen verloren gehen und so die Fehlerwahrscheinlichkeit der Risikoidentifikation steigen (Scandizzo 2005, 232).

Zudem kommt es aus Angst vor negativen Sanktionen vielfach zur Vertuschung von Schadensfällen oder Fehlern (Einhaus 2002, 490). Ferner realisieren Unternehmen bzw. Mitarbeiter zum Teil nicht, dass Risiken bestehen bzw. verhalten sich gegenüber diesen ignorierend. Problematisch ist dabei auch die Einführung neuer Produkte oder Prozesse, wenn technische Details oder das Umfeld nicht in vollem Umfang verstanden werden (Simons 1999, 92; Kimball 2000, 8). Insbesondere die Vermeidungshaltung bzw. hemmende Werte in der Unternehmenskultur beeinträchtigen die Vollständigkeit und Qualität der Risikoidentifikation negativ (DeMarco, Lister 2003, 123).

Ferner ist die Risikoidentifikation durch die Schwierigkeit charakterisiert, dass sie unter dem Wissen erfolgt, dass nicht alle Risiken erkannt werden können, aber trotzdem versucht werden muss, so viele Risiken wie möglich zu erfassen (Leidinger 2002, 242). Aus diesem Grund kommt der Definition eines Abbruchkriteriums eine große Bedeutung zu, da der betriebene Aufwand mit den Auswirkungen potentiell unentdeckter Risiken abgewogen werden muss (Gleißner 2001, 114; Faisst, Kovacs 2002, 11).

Speziell bei operationellen Risiken sind Probleme bei der Risikoidentifikation darauf zurückzuführen, dass sich Unternehmen vergleichsweise kurze Zeit mit dieser Risikokategorie auseinandersetzen. So ist bei operationellen Risiken im Vergleich zu anderen Risikokategorien wie Markt- oder Kreditrisi-

ken zu beachten, dass der Neuigkeitsgrad, die zum Teil hohe Komplexität sowie das zum Teil noch mangelnde Bewusstsein eine vollständige Identifikation aller bestehenden Risiken verhindern. Dies wird v.a. auch dadurch verstärkt, dass menschliches Fehlverhalten eine bedeutende Rolle bei operationellen Risiken einnimmt und sowohl deren Identifikation als auch Bewertung behindert (Jovic, Piaz 2001, 924; Füser et al. 2002, 497).

3.5.3 Risikobewertung

Als informatorische Grundlage des RM werden die Risikoidentifikation und die -bewertung durch die drei Fragen (1) „Was kann passieren?“, (2) „Wie wahrscheinlich ist es, dass dies passiert?“ und (3) „Was sind die Konsequenzen?“ geleitet (Kaplan, Garrick 1981, 13). Während die erste Frage Gegenstand der in Abschnitt 3.5.2 dargestellten Risikoidentifikation ist und auf die Risikoereignisse abstellt, zielen die beiden anderen Fragen auf die Eintrittswahrscheinlichkeit und das Schadensausmaß des Ereignisses ab, deren Ermittlung den Gegenstand der Risikobewertung darstellt. Insgesamt besteht das Hauptziel der Risikobewertung darin, die Voraussetzung für eine Steuerung der Risiken zu schaffen (Buhr 2000, 202). Dabei wird die Risikobewertung als zielgerichtete Analyse, Bewertung und Klassifizierung unternehmensinterner und -externer Risikopotentiale verstanden, die als Ergebnis Risiken hinsichtlich ihres Gefährdungspotentials in eine Rangordnung bringt bzw. in ein unternehmensindividuelles Risikoportfolio überführt (Romeike 2002, 15; Diederichs et al. 2004, 192).

In diesem Abschnitt werden zunächst die Größen Eintrittswahrscheinlichkeit und Schadensausmaß, auf deren Basis ein Erwartungswert gebildet wird, erörtert. Daraufhin wird auf verschiedene Ansätze zur Bewertung und die damit verbundenen Bewertungsprobleme eingegangen. Zudem sind die Beachtung von Interdependenzen zwischen den einzelnen Risiken ebenso wie deren Aggregation zu einer Gesamtrisikoposition Gegenstände der Risikobewertung, die in diesem Abschnitt erörtert werden.

Risiken sind durch Unsicherheit bezüglich des Eintritts von Ereignissen bzw. Umweltzuständen gekennzeichnet. Dennoch lassen sich ihnen objektiv oder subjektiv Wahrscheinlichkeiten zuordnen, die auf statistischen Verfahren, Erwartungen oder Expertise beruhen (Hermann 1996, 11). Während nach enger Auslegung das Vorhandensein objektiver Wahrscheinlichkeiten als erforderlich angesehen wird, werden nach einer weiten Auffassung auch subjektive Wahrscheinlichkeiten zur Spezifizierung des Risikos zugelassen (Karten 1972, 158ff; Hölscher 1987, 5).

Statistisch betrachtet kann die Eintrittswahrscheinlichkeit aus dem Verhältnis der günstigen zu den möglichen Ereignissen definiert werden. Dazu wird die Anzahl aller für eine bestimmte Menge günstigen Fälle d.h. aller Elemente aus einer Grundgesamtheit, die eine bestimmte Eigenschaft aufweisen, durch die Anzahl der möglichen Fälle, d.h. die Grundgesamtheit, dividiert (Hippmann 1997, 186). Da es vielfach nicht möglich ist, alle Elementarereignisse zu erfassen, kann eine statistische Bestimmung der empirischen Wahrscheinlichkeit erfolgen, die auf vergangenen Beobachtungen bzgl. der Realisie-

rungen eines Ereignisses aufsetzt. Dazu wird die Anzahl der günstigen Fälle durch die gesamte Anzahl der Beobachtungen dividiert, wobei diese Vorgehensweise ihre Rechtfertigung im Gesetz der großen Zahlen findet (Wetzel 1973, 33ff; Hippmann 1997, 186). Neben der statistischen Ermittlung der Wahrscheinlichkeit kann eine logische beziehungsweise subjektive Bestimmung der Wahrscheinlichkeit vorgenommen werden. Erstere basiert allein auf logischen Überlegungen und umfasst keine Versuche oder Erhebungen. Sie wird auch als objektive a-priori Wahrscheinlichkeit bezeichnet. Eine subjektive Ermittlung der Eintrittswahrscheinlichkeit beruht allein auf der Einschätzung von Menschen und kommt dann zum Tragen, wenn es nicht möglich ist, gleichmögliche Elementarereignisse zu formulieren. Diese Form wird auch als subjektive a-priori Wahrscheinlichkeit bezeichnet (Hochstädter 1989, 284).

Im Falle der subjektiven Einschätzung von Eintrittswahrscheinlichkeiten wird oftmals auf verbale Ausdrücke anstelle von Zahlen zurückgegriffen. Dies wird damit begründet, dass Zahlen eine scheinbare Genauigkeit vorspiegeln. Qualitative Aussagen sind vom Menschen einfacher und schneller zu erfassen als quantitative Werte und können durch Hinterlegung entsprechender Kategorien quantifiziert werden (Klett 1993, 28ff)[85]. Die Angabe einer Eintrittswahrscheinlichkeit erfordert in jedem Fall auch die Angabe eines Zeitraumes als Bezugsgröße z.B. ein Tag, ein Jahr oder eine Dekade, da ansonsten Aussagekraft fehlt (Gleißner 2001, 256; Schmitting, Siemes 2003, 534).

Im Hinblick auf das Schadensausmaß können mögliche Risiken monetären, qualitativen und reputationsbezogenen Charakter aufweisen. Erstere schlagen sich in der Form von Kapital-, Wertverlusten, Kostenerhöhungen oder entgangenem Gewinn direkt in der Gewinn- und Verlustrechnung nieder. Qualitative Risiken wirken sich indirekt durch verminderte Leistung aus, während Imagerisiken zu einer geänderten öffentlichen Meinung gegenüber dem Unternehmen führen und so langfristig finanzielle Auswirkungen nach sich ziehen (van den Brink 2001, 4; Seibold 2006, 19). Insbesondere bei qualitativen und Imagerisiken fällt die Quantifizierung des Schadensausmaßes schwer. Zudem muss beachtet werden, dass Folgeschäden hervorgerufen werden können oder durch das gleichzeitige Auftreten mehrerer Risiken das Schadensausmaß überproportional ansteigen kann. Bei der Ermittlung des Schadensausmaßes, sollte eine Anlehnung an Größen, wie z.B. Umsatz, Cash Flow oder EBIT des jeweiligen Unternehmens, erfolgen, um auf dieser Basis den maximal tragbaren Schaden zu identifizieren (Erdenberger 2001, 15; Junginger, Krcmar 2003, 20).

Auf der Basis einer Bezugsgröße kann eine Einteilung in verschiedene Schadensklassen erfolgen und beispielsweise eine fünfstufige Kategorisierung in Katastrophen-, Groß-, mittlere, Klein- und Bagatellschäden vorgenommen werden (Hermann 1996, 24f; Erdenberger 2001, 15; Leidinger 2002, 247).

[85] Neben verbalen Aussagen können alternativ zur numerischen Bewertung von Risken auch graphische Hilfsmittel wie Zeitpläne etc. herangezogen werden, da auch eine solche Abschätzung vielfach leichter fällt als eine prozentuale Darstellung (DeMarco, Lister 2003, 86).

Nach ISO/IEC Guide 51:1999[86] ergibt sich nach Definition 3.2 ein Risiko aus Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und dessen Schweregrad. Dieses Produkt wird in der Literatur überwiegend als Erwartungswert (Erdenberger 2001, 15; Gleißner, Meier 2001, 56) und zum Teil auch als Risikopotential, Tragweite oder Risikograd bezeichnet (Hermann 1996, 24; Romeike 2004b, 112f)[87] [88].

Speziell operationelle Risiken treten vielfach auch in extremen Ausprägungen auf, die entweder durch eine geringe Eintrittswahrscheinlichkeit und ein hohes Schadensausmaß gekennzeichnet sind oder sehr häufig auftreten und mit vergleichsweise geringem Schaden verbunden sind. Erstere werden auch kurz LFHI-Risiken (Low Frequency High Impact) und letztere als HFLI-Risiken (High Frequency Low Impact) bezeichnet. Zudem bestehen auch Risiken, die Ausprägungen zwischen den Extremen annehmen (Piaz 2002, 50f; Jorion 2003, 546; Locher et al. 2004, 11; Ayliffe 2005, 48ff). Charakteristisch für LFHI-Risiken sind dabei Naturkatastrophen oder Brände. Auf einer Gesamtrisikoebene können sich LFHI-Risiken aber auch aus der Verkettung verschiedener Risikoereignisse ergeben. HFLI-Risiken wie Betrug oder menschliche Fehler sind die am häufigsten auftretenden operationellen Risiken, wobei zu beachten ist, dass diese auch gerade in ihrer Aggregation ein hohes Schadensausmaß aufweisen können. In der Praxis erfolgt eine Konzentration auf LFHI-Risiken, obwohl aus Sicht des Qualitätsmanagements von Prozessen insbesondere auch HFLI wertvolle Informationen liefern können und erhebliche Auswirkungen aufweisen können. Innerhalb dieser Unterteilung variieren operationelle Risiken auch im Hinblick auf die Entdeckungswahrscheinlichkeit (Piaz 2002, 51f; Locher et al. 2004, 23).

Die Erwartungswertberechnung hat zum Problem, dass ganz unterschiedliche Risiken gleich eingestuft werden (Locher 2004, 12). So ergibt sich für Risiken, die z.B. alle 100 Jahre eintreten, dafür aber mit einem sehr hohen Schaden einhergehen unter Umständen derselbe Erwartungswert, wie für Risiken, die vielfach im Jahr auftreten und vergleichsweise geringe Schäden nach sich ziehen (Locher 2004, 12). Füser et al. schlagen vor, diese Gleichbehandlung von sehr unterschiedlichen Risiken dadurch zu vermeiden und die Aussagekraft zu erhöhen, indem ein zeitraumbezogener bzw. annualisier-

[86] ISO/IEC Guide 51:1999 ist eine technische Regel und wird in der Langform als „Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen“ bezeichnet.

[87] Dabei entspricht der Erwartungswert nicht den tatsächlichen Kosten, die anfallen, wenn ein Risiko eintritt, sondern diese sind bezogen auf den Einzelfall höher. Wenn z.B. ein Schaden von 2 Mio. € mit einer Wahrscheinlichkeit von 0,5% eintritt, so ergibt sich ein Erwartungswert von 100.000 €. Realisiert sich das Risiko tatsächlich, so sind allerdings 2 Mio. € erforderlich, um den Schaden zu beheben. Da im gesamten Risikoportfolio eines Unternehmens einige erwartete Risiken eintreten und andere nicht, gleicht sich der Erwartungswert über alle Risiken in der Regel aus (DeMarco, Lister 2003, 66f).

[88] Alternativ zur Sicht des Risikos als Erwartungswert kann aus statistischer Sicht Risiko aus der Variabilität der Ergebnisse (d.h. Wahrscheinlichkeits- oder Dichtefunktion einer Zufallsvariable) bestimmt werden. Nach dieser Sichtweise wird das Risiko nicht durch den Erwartungswert selbst, sondern durch die Streuung um den Erwartungswert beschrieben. Umso größer die Varianz ist, desto größer ist die Gefahr einer Abweichung, wobei eine positive Abweichung eine Chance (upside risk) und eine negative Abweichung ein Risiko (downside risk) bezeichnet. Somit stellt die Varianz ein zweiseitiges Risikomaß dar, das vorwiegend im finanzwirtschaftlichen Bereich Anwendung findet und auch als Volatilität bezeichnet wird (Oehler, Unser 2002, 11ff; Culp, Mensink 2003, 99f).

ter Erwartungswert gebildet wird. Dabei wird das Schadensausmaß mit dem erwarteten Eintritt in einem Jahr in Beziehung gesetzt. Tritt ein bestimmtes Risiko z.B. alle 10 Jahre auf, so wird der entstehende Schaden durch 10 dividiert und somit auf den Zeitraum eines Jahres umgelegt. Geht man davon aus, dass die Schäden unabhängig voneinander eintreten, so können die einzelnen Risiken aufaddiert werden (Füser et al. 2002, 498).

Insgesamt wird die Bestimmung des Erwartungswertes durch die vorhandene Datengrundlage limitiert. So ist im Falle einer vollständigen Datengrundlage eine quantitative Bestimmung mittels Methoden der Wahrscheinlichkeitsrechnung oder empirischen Verlustverteilungen möglich. Bei einer unvollständigen Datengrundlage ist eine rein quantitative Bestimmung nicht mehr möglich und die Zuhilfenahme subjektiver Bewertungsansätze (z.B. Benchmarking) erforderlich. Bei einer fehlenden Datengrundlage ist nur eine rein qualitative Bewertung z.B. mittels Experteninterviews bzw. -einschätzung möglich (Füser et al. 2002, 498). Diese wird dadurch verbessert, dass die subjektiven Daten von Experten diskutiert und detailliert begründet sowie die Schätzungen nachträglich nochmals auf ihre Plausibilität geprüft werden (Gleißner 2001, 112). Dieses Problem tritt vorwiegend auch bei operationellen Risiken auf, da Bewertungsverfahren noch am Anfang stehen und in der Regel Vergangenheitsdaten nicht in entsprechendem Ausmaß vorliegen (Jovic, Piaz 2001, 924; Romeike 2002, 15). Dennoch sollte auch bei großen Unsicherheiten eine Nichtquantifizierung von Risiken die Ausnahme bleiben und soweit als möglich eine Bewertung vorgenommen werden. Falls dies quantitativ nicht möglich ist, können neben einer qualitativen Bewertung auch Best- und Worst-Case Szenarien herangezogen werden (Diederichs et al. 2004, 192f).

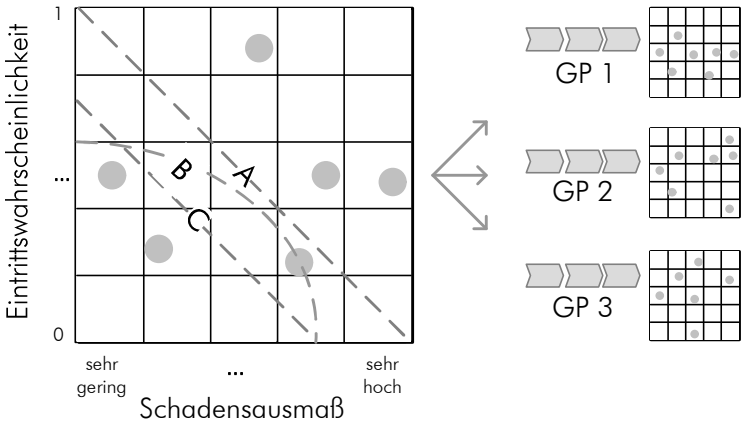


Abb. 13 Risiko-Portfolio

Zudem ist bei der Bewertung darauf zu achten, dass ein einheitlicher Bewertungsmaßstab (z.B. Umsatz, Gewinn) angewandt wird, um die Vergleichbarkeit der Risiken zu gewährleisten (Schulte 1997, 12; Erdenberger 2001, 15; Gleißner 2001, 255; Romeike 2002, 15). Eine Positionierung von Risiken kann beispielsweise vorgenommen werden, indem man deren Eintrittswahrscheinlichkeiten, die linear in Schritten von 0,2 steigen und Schäden, die im Hinblick auf ihre Schwere ansteigen, abträgt. Die Dringlichkeit einer vertiefenden Betrachtung bzw. Steuerung wird dabei durch die unternehmensspezifische Risikoschwelle, die auch als Risikoakzeptanzlinie bezeichnet wird, determiniert (Hornung et al. 1999, 321; Leidinger 2002, 246f; Romeike 2002, 15; von Hohnhorst 2002, 102f). Da die Risiko-

schwellen mit der unternehmensindividuellen Risikoneigung variieren, sind exemplarisch drei mit A, B und C bezeichnete Risikoschwellen in Abb. 13 dargestellt. Eine derartige Zuordnung von Risiken kann auch in einer feineren Granularität erfolgen, indem die anhand der beiden Parameter beschriebenen Risiken einzelnen Geschäftsprozessen bzw. deren Phasen zugewiesen werden. Dadurch können qualitative Informationen gewonnen werden, in welchen Prozessphasen ein besonders hohes Risikopotential vorhanden ist. Auf dieser Basis kann dann eine entsprechend intensivere Analyse des Geschäftsprozesses erfolgen (Scandizzo 2005, 232). Diese Disaggregation in Risiko-Portfolios für die verschiedenen Geschäftsprozesse (GP 1, 2, 3) ist ebenfalls in Abb. 13 dargestellt.

Eine derartige Einordnung der Risiken dient allerdings nur zu einer groben Erstbewertung und zur Priorisierung und hat somit eine Art Filterfunktion, mittels derer bestimmt wird, welche Risiken im Folgenden einer detaillierten Betrachtung unterzogen werden (Gleißner, Romeike 2005, 201). Die detaillierte Betrachtung der priorisert zu betrachtenden Risiken erfolgt dabei durch die Angabe einer entsprechenden Verteilungsfunktion (z.B. Normal-, Poisson- oder Binomialverteilung), auf deren Basis weitere Analysen vorgenommen werden können. Die Ermittlung der Parameter der Verteilungsfunktion kann durch verschiedene Methoden und Instrumente gestützt werden, die nachfolgend erläutert werden. Faisst und Kovacs führen Befragungstechniken, Indikator-Ansätze, stochastische Methoden und Kausal-Methoden als mögliche Ansätze zur Quantifizierung an (Faisst, Kovacs 2003, 342ff), während Gleißner und Romeike statistische Analysen, Benchmarks, Expertenschätzungen und sonstige Methoden unterscheiden (Gleißner, Romeike 2005, 207ff)[89]. Neben einer quantitativen und qualitativen Einordnung der Methoden, kann diese auch im Hinblick auf ihre Ansatzpunkte Bottom-up und Top-down erfolgen. Dabei gehen Top-down Methoden bei der Betrachtung des Risikos vom Schaden, der aus dem Eintritt des Risikoereignisses resultiert, aus, während Bottom-up Methoden an den Ursachen ansetzen und versuchen, daraus die Folgen abzuleiten (Jovic, Piaz 2001, 924; Romeike 2004b, 103ff). Nachfolgend werden für die entsprechenden Kategorien einige Methoden dargestellt, um so einen Überblick über die verschiedenen Bewertungsverfahren im RM zu geben, wobei die Unterteilung von Faisst und Kovacs primär zugrunde gelegt und um Aspekte alternativer Gliederungen ergänzt wird.

Befragungstechniken: Im Rahmen von Befragungstechniken wird versucht entweder schriftlich (z.B. strukturierte Fragebögen) oder mündlich (z.B. Interviews, Workshops) mittels qualitativer Fragen Rückschlüsse auf die Höhe möglicher Schäden zu ziehen (Faisst, Kovacs 2003, 342ff). Auch die von Gleißner und Romeike angegebenen Expertenschätzungen können dieser Kategorie zugeordnet werden. Die Befragungen zielen dabei darauf ab, die zur Aufstellung der Verteilungen erforderlichen Parameter zu bestimmen, wobei die Nachteile qualitativer Verfahren im Hinblick auf Subjektivität und Qualität zum Tragen kommen können. Delphi-Studien stellen unter Einbezug mehrerer Experten ein

[89] Eine ähnliche Klassifikation ist zudem bei Jorion (2003, 540f) zu finden.

mehrstufiges Verfahren zur Abschätzung der Parameter dar und weisen eine vergleichsweise höhere Verlässlichkeit auf (Gleißner, Romeike 2005, 208). Methoden dieser Kategorie setzen in der Regel Bottom-up an und sind qualitativer Natur (Jovic, Piaz 2001, 925; Romeike 2004b, 104).

Indikator-Ansätze: Bei einem Indikator-Ansatz wird eine Kennzahl oder ein Kennzahlensystem herangezogen, um die Eintrittswahrscheinlichkeit und das Schadensausmaß der Risiken zu schätzen (Scandizzo 2005, 235). Basierend auf empirischen Untersuchungen und der Einschätzungen von Experten werden Indikatoren ausgewählt, die sich eignen, die Parameter des Risikos zu bestimmen (Faisst, Kovacs 2003, 342ff). Weite Verbreitung finden diese Ansätze im Rahmen von Basel II, um die Höhe des zu hinterlegenden Eigenkapitals zu bestimmen. So kann in diesem Kontext der Basis-Indikator-Ansatz herangezogen werden, nach dem der Bruttoertrag einer Bank mit einem Faktor multipliziert wird, der auf der Grundlage von empirischen Untersuchungen und unter Berücksichtigung von Sicherheitszuschlägen bestimmt wurde. Daneben werden durch den Baseler Bankenausschuss noch weitere Indikator-Ansätze wie der Standard-Ansatz oder der Internal-Measurement Ansatz als Verfahren angeboten (Basel 2005, 145ff). Im Rahmen von Kennzahlensystemen werden mehrere Indikatoren, die aus verschiedenen Quellen stammen (z.B. historische Schadensdaten, Systemausfallzeiten, Mitarbeiterfluktuation), betrachtet und zueinander in Beziehung gesetzt (Klomfass, Quadt 2001, 324f; Faisst, Kovacs 2003, 342ff). Diese Parameter, auch Key Risk Indicators (KRI) genannt, beziehen sich auf Geschäftsprozesse bzw. auf Bündel aus diesen und dienen dazu, Veränderungen in deren Risikoprofil vorherzusehen, wobei mittels regelmäßiger Messungen überprüft wird, ob vorgegebene Schwellenwerte überschritten wurden.

Stochastische Methoden: Diese Methoden legen Vergangenheitsdaten und entsprechende statistische Verteilungsfunktionen zur Bewertung operationeller Risiken zugrunde (Faisst, Kovacs 2003, 342ff). Eine der am weitesten verbreiteten Methoden im RM ist der Value-at-risk, wobei die Verbreitung insbesondere den Bereich der Marktrisiken betrifft, in der diese Methode einen Bewertungsstandard darstellt (Stickelmann 2002, 7). Mittlerweile findet diese Methode aber auch bei der Bewertung anderer Risikogruppen, wie z.B. den operationellen Risiken, Anwendung. Der Value-at-risk kann als „wahrscheinlicher Höchstschaden“ bezeichnet werden und ist definiert als der betragsmäßig maximale Verlust eines Risikoportfolios, der mit einer bestimmten Wahrscheinlichkeit innerhalb eines festgelegten Zeitraums nicht überschritten wird (Schierenbeck 1999, 14). Die vorgegebene Wahrscheinlichkeit bezeichnet man als Konfidenzniveau (α), auf dessen Basis Konfidenzintervalle ($1-\alpha$), die zumeist zwischen 0,95 und 0,99 liegen, gebildet werden. Diese sagen aus, dass mit einer Wahrscheinlichkeit von $1-\alpha$ (z.B. 95%) die wahre Lage des Parameters, also die durch den Value-at-risk ausgedrückte Schadenshöhe, nicht überschritten wird. Somit sinkt die Wahrscheinlichkeit der Überschreitung der maximalen Schadenshöhe mit abnehmendem α. Folglich gibt der Value-at-risk an, bis zu welchem Umfang

Abweichungen vom erwarteten Niveau realistisch sind und welcher Eigenkapitalbedarf für die Deckung möglicher Verluste besteht (Gleißner 2001, 258).

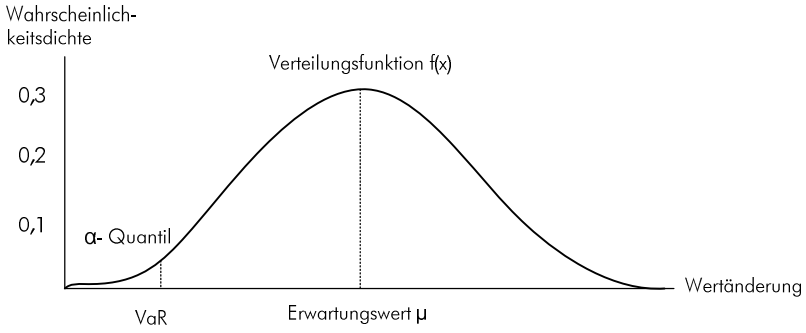


Abb. 14 Value-at-Risk

Der Value-at-risk kann als α-Quantil aus der Verteilungsfunktion abgelesen werden, wobei in Abb. 14 eine Normalverteilung unterstellt ist, die durch die Parameter Erwartungswert (μ) und Standardabweichung (σ) beschrieben wird. Diese Parameter können aus historischen Daten stammen oder mittels Schätzungen erhoben werden (Burger, Buchhart 2002, 121f)[90]. Der Value-at-risk kann mittels verschiedener Simulationsverfahren, wie z.B. der Monte-Carlo Simulation oder der historischen Simulation ebenso wie mithilfe der Delta Normal oder Delta Gamma Methode, die analytische Ansätze darstellen, ermittelt werden (Junginger et al. 2003, 360). Als weitere Bewertungsmethoden können Analysen von Risiko- bzw. Verlustdatenbanken oder die Extremwerttheorie[91] herangezogen werden. Methoden dieser Kategorie können als quantitative Top-down Ansätze eingeordnet werden (Jovic, Piaz 2001, 925; Romeike 2004b, 104).

Kausal-Methoden: Als weitere Kategorie stellen Kausal-Methoden auf die Analyse von Zusammenhängen zwischen Risikoquellen und den daraus resultierenden Schäden, also Ursache- und Wirkungsbeziehungen, ab und setzen dazu zum Teil statistische Methoden ein. Durch diese Beziehungen soll erklärt werden, welche Variablen eine oder mehrere bestimmte Variablen beeinflussen (Gleißner, Füser 2001, 188). Beispiele für Methoden sind Bayessche Netzwerke oder Neuronale Netze (Faisst, Kovacs 2003, 342ff). Ebenfalls zur Analyse von Ursachen können Fehlerbaumanalysen eingesetzt werden, mittels derer ausgehend vom Risikoereignis über mehrere Stufen hinweg dessen Ursachen und Bedingungen untersucht werden. Dabei besteht das Ziel darin, ursprüngliche Ereignisse zu identifizieren, deren Eintrittswahrscheinlichkeiten bekannt sind, um so die Eintrittswahrscheinlichkeit des Risikoereignisses auf der obersten Ebene zu bestimmen (Gleißner, Romeike 2005, 209). Derartige Methoden haben zum Vorteil, dass sie einen hohen Erklärungswert aufweisen. Die Ermittlung der Zusammenhänge zwischen den Variablen ist allerdings durch ein Kausalitätsproblem gekennzeichnet. Dies

[90] Speziell für die Bewertung operationeller Risiken bzw. Betriebsrisiken kann der Operational Value-at-risk eingesetzt werden, da dieser auch extreme Abweichungen, die sich durch die hohe Relevanz von HFLI- und LFHI-Risiken in diesem Bereich ergeben, entsprechend berücksichtigt. In diesem Fall werden nicht Normalverteilungen, sondern beispielsweise Poisson-, Weibull- oder Lognormal-Verteilungen zugrunde gelegt, da diese sich im Einzelfall vergleichsweise besser eignen, die tatsächliche Verteilung dieser spezifischen Schadensfälle darzustellen (Kirmße 2003). Dies liegt v.a. daran, dass positive und negative Abweichungen des Erwartungswertes von Schadensfällen nicht gleich verteilt sind, sondern für sehr negative Abweichungen ein größeres Risiko besteht.

[91] Siehe hiezu auch (Cruz 2002, 63).

bedeutet, dass aufgrund einer Korrelation zwischen Variablen nur bedingt auf eine Abhängigkeit geschlossen werden kann, da diese von weiteren Einflussfaktoren oder dem Zufall (z.B. Schein- oder zufällige Korrelation) determiniert werden kann (Gleißner, Füser 2001, 188).

Nach der Bewertung der Einzelrisiken erfolgt unter Beachtung der Interdependenzen deren Aggregation, um die Gesamtrisikoposition des Unternehmens zu bestimmen. Dabei ist insbesondere eine vernetzte Betrachtung der Risiken bedeutend, da durch die Interdependenzen zwischen den Risiken die Eintrittswahrscheinlichkeiten und Schadensausmaße variieren und sich so sowohl kumulative als auch kompensierende Wechselwirkungen ergeben können (Gleißner 2001, 255; Romeike 2004a, 43; Schmitting, Siemes 2004, 104; Thomson 2005, 134). Karten weist darauf hin, dass betriebliche Einzelrisiken zwar vielfach voneinander unabhängig, aber nicht vollständig positiv korreliert sind. Dies hat zur Folge, dass im Hinblick auf die Gesamtrisikoposition Ausgleichseffekte bestehen (Karten 1993, Sp 3828). Interdependenzen können als positive bzw. negative Korrelationen zwischen den Risiken spezifiziert werden (Thomson 2005, 134). Dabei können bezogen auf zwei Risiken verschiedene Arten von Interdependenzen unterschieden werden (Schmitting, Siemes 2003, 535ff). So bezeichnen Risikoantinomien den Fall, dass sich zwei Risikoereignisse gegenseitig ausschließen, was zur Folge hat, dass der Eintritt eines Risikoereignisses die Realisierung eines anderen unmöglich macht. Risikokonkurrenz als Interdependenz kann dazu führen, dass der Eintritt eines Risikoereignisses die Eintrittswahrscheinlichkeit eines anderen verbundenen Ereignisses vermindert. Risikokomplementarität bezeichnet den umgekehrten Fall, was bedeutet, dass mit dem Eintritt eines Risikos auch zugleich die Eintrittswahrscheinlichkeit eines anderen ansteigt bzw. Erhöhungen oder Verminderungen der Eintrittswahrscheinlichkeiten zweier Risiken gleichlaufend sind. In diesem Kontext ist auch das Auftreten von Kumulationsrisiken von Bedeutung, die aus sich verstärkenden Interdependenzen entstehen können (Happel, Liebewein 2000, 5). Von Risikoindifferenz wird dann gesprochen, wenn sich zwei Risiken gegenseitig nicht beeinflussen, diese also unabhängig voneinander sind (Schmitting, Siemes 2003, 535ff). Über die Betrachtung von zwei Risiken hinausgehend, können unter Einbezug mehrerer Risiken weitere komplexere Szenarien beschrieben werden, die die verschiedenen Arten von Interdependenzen einschließen.

Aufgrund der bestehenden Interdependenzen ist die Aggregation der Einzelrisiken komplex. Im Bereich der finanziellen Risiken wird in der Praxis zum Teil eine additive Aggregation von Risiken vorgenommen (Schulte 1997, 26). Ein derartiges Vorgehen unterstellt allerdings die Unabhängigkeit der Risiken. Da dies eher selten der Fall ist, sind bei der Aggregation Interdependenzen zu berücksichtigen, da eine Nichtbeachtung aufgrund kumulativer oder kompensatorischer Effekte dazu führen kann, dass die Gesamtrisikoposition des Unternehmens falsch ausgewiesen wird (Schulte 1997, 27; Schmitting, Siemes 2003, 535; Romeike 2004a, 44).

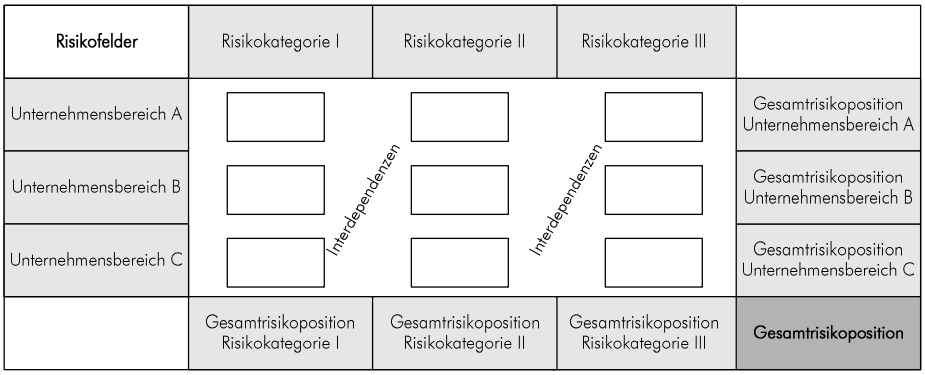


Abb. 15 Matrix zur Risikoaggregation

Die Aggregation der Risiken kann über verschiedene Stufen hinweg erfolgen. Auf der obersten Stufe können sämtliche Risiken in einer Gesamtrisikoposition des Unternehmens ausgedrückt werden. Auf darunter liegenden Aggregationsebenen können einerseits Risiken verschiedener Kategorien über Unternehmensbereiche, wie z.B. Vertrieb,[92] aggregiert werden und so eine entsprechende Gesamtrisikoposition für den jeweiligen Unternehmensbereich ermittelt werden. Zum anderen können auch Gesamtrisikopositionen für einzelne Risikokategorien z.B. leistungswirtschaftliche Risiken (siehe Abb. 10) über alle Unternehmensbereiche ermittelt werden (Kuhn 2002, 164f; Junginger et al. 2003, 361). Diese Sachverhalte sind anhand der in Abb. 15 dargestellten Matrix zur Risikoaggregation veranschaulicht.

Neben der Ermittlung der Gesamtrisikoposition ist es auch zweckmäßig, die relative Bedeutung der Einzelrisiken zu ermitteln. Dies kann mithilfe von Sensitivitätsanalysen erfolgen (Gleißner 2001, 125; Romeike 2004a, 44). Da die Aggregation in der Praxis zum Teil mit Schwierigkeiten verbunden ist, wird sie oftmals vernachlässigt oder ungeeignet gelöst. Ein mögliches Verfahren zur Aggregation ist die Monte-Carlo Simulation, nach der verschiedene durch Wahrscheinlichkeitsverteilungen beschriebene Einzelrisiken, wie z.B. Zins- oder Materialpreisänderungen, in einem Rechenmodell korrespondierenden Positionen der Bilanz oder der Gewinn- und Verlustrechnung (z.B. Zinsaufwand oder Materialkosten) zugewiesen werden. Mittels einer Vielzahl an Simulationsläufen wird ein bestimmter Zeitraum (z.B. ein Geschäftjahr) simuliert und die entsprechenden Positionen in Bilanz oder GuV errechnet. Je Simulationslauf ergibt sich auch ein Wert für entsprechende Zielgrößen wie das Betriebsergebnis oder der Gewinn vor Steuern. Auf diese Weise erfolgt eine Näherung der Aggregation der verschiedenen Verteilungen durch eine entsprechend hohe Anzahl an Simulationsläufen. Als Ergebnis erhält man eine Wahrscheinlichkeitsverteilung der Gesamtrisikoposition, aus der auch der unter den stochastischen Methoden zur Bewertung dargestellte Value-at-risk als entsprechendes Quantil des Konfidenzintervalls abgelesen werden kann (Gleißner 2001, 126ff).

Nicht alle Risiken und im Speziellen operationelle Risiken sind vollständig quantifizierbar, was auf eine Reihe von Bewertungsproblemen zurückgeführt werden kann (Young 1999, 10; Hirschmann,

[92] In diesem Fall kann eine Anlehnung an die Primär- bzw. Sekundäraktivitäten der Wertschöpfungskette erfolgen (Porter 1985, 36ff) bzw. ein entsprechendes Organigramm bzw. die Aufbauorganisation des Unternehmens zugrunde gelegt werden.

Romeike 2004, 14). So kommen diese Probleme zum einen dadurch zustande, dass die Umfeldbedingungen nicht statisch sind, sondern vielmehr dynamisch die Eintrittswahrscheinlichkeit und das Schadensausmaß der Risiken beeinflussen (Füser et al. 2002, 498; Locher 2004, 22). Zum anderen weisen operationelle Risiken vielfach eine hohe Komplexität auf. So können Parameter zur Beschreibung menschlichen Fehlverhaltens nur schwer erfasst werden (Young 1999, 10). Ferner können Bewertungsprobleme darauf zurückzuführen sein, dass z.B. aufgrund des Neuigkeitsgrades keine Erfahrungswerte vorliegen oder die Langfristigkeit des zugrunde liegenden Zeithorizontes die Bestimmung ihrer Risikoverteilungen einschränkt, was insbesondere auf strategische Risiken zutrifft (Schulte 1997, 15). Insbesondere bei operationellen Risiken liegen in der Regel keine oder nur unzureichende Vergangenheitsdaten vor und sind zudem von der Qualität der internen Prozesse abhängig (Santomero 2003, 4; Locher 2004, 22; Wolf 2005, 73).

Die Bewertung von Verlusten bzw. Schäden wird zusätzlich dadurch erschwert, dass sich diese nicht nur direkt, sondern auch indirekt auswirken können (Tiebing 2004, 35). Selbst bei Vorliegen von Vergangenheitsdaten behindert ein idiosynkratischer Charakter der Risiken deren Anwendung (Williams et al. 2006, 73). Dies trifft auf operationelle Risiken in besonderem Maße zu. Dennoch ist der Aufbau von Verlustdatenbanken im Bereich der operationellen Risiken erforderlich, um eine verbesserte Analyse durchführen zu können und primär quantitative anstelle qualitativer Bewertungsverfahren zugrunde legen zu können (Faisst et al. 2002, 22ff). Weiterhin wird gemäß § 286 SolvV[93] gefordert, dass bei der Bestimmung des Anrechnungsbetrages für operationelle Risiken interne Schadensdaten der letzten fünf Jahre verwendet werden. Darüber hinaus sind auch Initiativen von Bedeutung, die die unternehmensübergreifende Sammlung von Verlustdaten und die anonymisierte Bereitstellung zum Gegenstand haben, wobei diese Datenbanken in Bezug auf operationelle Risiken insbesondere für HFLI und LFHI Risiken relevant sind. Initiativen, die auf eine gemeinsame Datenbank zu operationellen Risiken abzielen, gehen z.B. von BBA[94] und GARP[95] aus (Stickelmann 2002, 10).

Ein weiteres Problem bezüglich der Betrachtung von Risiken ist darin zu sehen, dass Einzelrisiken isoliert betrachtet keine nennenswerte Bedeutung aufweisen, aber in Kumulation mit anderen Risiken eine erhebliche Bestandsgefährdung darstellen können (Wall 2001, 219; Romeike 2004a, 44). Die Prognose der Interdependenzen und die potentielle Kumulation gestalten sich als eine äußerst komplexe Aufgabe im RM.

[93] SolvV steht für Solvabilitätsverordnung. Siehe hierzu auch Abschnitt 3.6.2.
[94] BBA steht für British Bankers' Association (www.bba.org.uk).
[95] GARP steht für Global Association of Risk Professionals (www.garp.com).

3.5.4 Risikosteuerung

Nach der Betrachtung der Risikoidentifikation und -bewertung werden in diesem Abschnitt die Ziele der Risikosteuerung, die verschiedenen Handlungsalternativen, die Möglichkeiten der Priorisierung und Limitationen erörtert.

Das primäre Ziel der Risikosteuerung besteht darin, mittels verschiedener Maßnahmen eine gezielte Beeinflussung aller wesentlichen Risiken zu erreichen. Dadurch soll die Gesamtrisikoposition des Unternehmens auf ein tragbares und akzeptables Niveau reduziert werden und somit ein ausgewogenes Verhältnis zwischen Chancen und Risiken erreicht werden. Basierend auf den Ergebnissen der Risikoidentifikation und -bewertung wird im Rahmen der Risikosteuerung vor dem Hintergrund der Verlustobergrenze entschieden, ob die Risiken getragen werden oder die Einleitung von Steuerungsmaßnahmen erforderlich ist (PWC 2001, 20; Romeike 2002, 16; Diederichs et al. 2004, 193). Das maximale Risikodeckungspotential wird durch die laufende Ertragskraft und die bestehenden Eigenkapitalreserven bestimmt. Schulte nimmt eine feinere Abgrenzung in primäres, sekundäres und tertiäres Risikodeckungspotential vor, wobei ersteres zur regelmäßigen Deckung von Verlusten herangezogen wird und beispielsweise kalkulierte Risikokosten oder -prämien umfasst. Das sekundäre Risikodeckungspotential wird herangezogen, wenn das primäre aufgebraucht ist und schließt z.B. den strukturellen Mindestgewinn oder stille Zwangsreserven ein. Zuletzt wird das tertiäre Risikodeckungspotential, das Eigenkapital bzw. Eigenkapitalsurrogate umfasst, zum Ausgleich der Verluste verwendet (Schulte 1997, 28ff).

Die Steuerungsmaßnahmen können sowohl an den Ursachen als auch an den Wirkungen der Risiken ansetzen, was bedeutet, dass die Maßnahmen im ursachenorientierten Fall auf die Reduzierung der Eintrittswahrscheinlichkeit des Risikos abzielen und im wirkungsbezogenen Fall eine Reduzierung des Schadensausmaßes erreicht werden soll (Gleißner 2001, 258; von Hohnhorst 2002, 102; Jorion 2003, 539; Andersson, Norrman 2004, 163).

Bei einer zeitlichen Abgrenzung kann zwischen proaktiven und reaktiven Maßnahmen unterschieden werden. Während erstere zur Reduktion der Eintrittswahrscheinlichkeit und des Schadensausmaßes vor Eintritt der Risiken ergriffen werden, dienen reaktive Maßnahmen zur Bekämpfung bereits eingetretener Risiken und haben keinerlei Einfluss auf die Eintrittswahrscheinlichkeit, sondern nur auf das Schadensausmaß (Lück et al. 2002, 231; Schmitting, Siemes 2004, 104f). In den letzten Jahren hat die proaktive Ausrichtung des RM zugenommen, da die ex post Bewältigung von Risiken oftmals mit hohen Aufwänden verbunden ist und somit reaktives RM eine vergleichsweise geringere Werthaltigkeit aufweist (Hornung et al. 1999, 318f; Kubitscheck 2000, 39; Romeike 2002, 14).

Hinsichtlich der Risikosteuerung besteht in der Literatur weitgehend Einigkeit, dass Vermeiden, Vermindern, Überwälzen und Akzeptieren die vier primären Handlungsalternativen darstellen (Wyss 2000, 179f; Gleißner, Meier 2001, 58; PWC 2001, 20; Gleißner 2001, 258; Diederichs et al. 2004,

193). Speziell im interorganisationalen Bereich wird zudem die Risikoteilung als weitere Alternative genannt (Norrman, Lindroth 2004, 22). Der Gegenstand dieser verschiedenen Handlungsalternativen wird nachfolgend detaillierter betrachtet.

Vermeiden: Bei der Handlungsalternative Vermeiden werden risikobehaftete Geschäfte bzw. Aktivitäten nicht eingegangen bzw. unterlassen. Dies kann unter Umständen das Beenden eines Projektes, den Rückzug aus einem Markt oder in einer extremen Ausprägung die Einstellung des Geschäftsbetriebes bedeuten (DeMarco, Lister 2003, 63; Gorrod 2004, 12; Williams et al. 2006, 71). Die Risikovermeidung führt somit im Extremfall zu einem Restrisiko von Null (Junginger, Krcmar 2003, 20). Dabei ist diese Alternative dann relevant, wenn die Aktivitäten existenzielle Risiken nach sich ziehen, wobei Risikovermeidung in der Regel nur dann ergriffen wird, wenn keine anderen Alternativen zur Risikosteuerung zur Verfügung stehen bzw. deren Wirksamkeit zu gering ist (Hornung et al. 1999, 321; Piaz 2002, 144; Diederichs et al. 2004, 193). Da eine Vermeidung vielfach einer Abschottung oder der Geschäftsaufgabe gleichkäme, ist diese Alternative oftmals keine wirkliche Option bzw. ökonomisch nicht sinnvoll (Claflin 2001, 2; Lux, Peske 2002, 154). Dies trifft v.a. auch auf operationelle Risiken zu, da die operativen Geschäftsprozesse die Basis der Wertschöpfung darstellen und folglich ausgeführt werden müssen (Wyss 2000, 179f; Einhaus 2002, 490).

Vermindern: Im Gegensatz zur Risikovermeidung wird bei der -verminderung das Geschäft eingegangen bzw. die Aktivität durchgeführt und den identifizierten Risiken Steuerungsmaßnahmen entgegengesetzt, die das Risiko aber nicht vollständig ausschalten (Hornung et al. 1999, 321; Wyss 2000, 179f; Diederichs et al. 2004, 193). Diese Strategie betrifft vorwiegend Risiken, deren Risikoklasse als hoch oder mittel eingestuft wird (Junginger, Krcmar 2003, 20). Mittels verschiedener Maßnahmen kann versucht werden, die Eintrittswahrscheinlichkeit des Schadens oder das Ausmaß des Schadens zu reduzieren. Dabei sind derartige Maßnahmen in der Regel nicht auf der Ebene der Einzelrisiken angesiedelt, sondern betreffen bestimmte Gruppen an Risiken (DeMarco, Lister 2003, 63). Die Maßnahmen der Risikoverminderung können organisatorischer, technischer oder rechtlicher Natur sein[96]. So können beispielsweise Frühwarnsysteme eingerichtet werden oder in Prozessen zusätzliche Kontrollmaßnahmen implementiert werden, um Risiken zu identifizieren. Zudem können Richtlinien und Verfahrensanweisungen eingesetzt sowie spezifische Sensibilisierungsmaßnahmen für Mitarbeiter ergriffen werden, um das Risikopotential bereits erkannter Risiken zu reduzieren (Einhaus 2002, 490; Piaz 2002, 149ff; Williams et al. 2006, 71). Einige Autoren sehen in der Diversifikation von Risiken eine eigene Handlungsalternative (Schulte 1997, 17; Williams et al. 2006, 71), wobei hier die Auffassung vertreten wird, dass die Diversifikation in diesem Kontext lediglich einen Sonderfall der Risikoverminderung darstellt (Piaz 2002, 145). Diversifikation bezeichnet die bewusste Ausnutzung der Risikostreuung, die zu einem Ausgleich von Chancen und Risiken führt, also kompensatorische Effekte

[96] Für Details zur Kategorisierung von Steuerungsmaßnahmen siehe auch Abschnitt 5.10.1.

aufweist (Schulte 1997, 17). Dabei ist die Diversifikation v.a. im Bereich der Marktrisiken gebräuchlich (Williams et al. 2006, 71).

Überwälzen: Die Handlungsalternative Überwälzung zielt rein auf die Reduktion des potentiell eintretenden Schadens ab, indem die einzugehenden Risiken vollständig oder teilweise auf andere Wirtschaftssubjekte vor Eintritt des Schadens übertragen werden (Einhaus 2002, 490; Diederichs et al. 2004, 193). Dabei werden für ausgewählte Risiken Versicherungen abgeschlossen, sofern deren Versicherbarkeit gegeben ist (Einhaus 2002, 490; Junginger, Krcmar 2003, 20; Williams et al. 2006, 71). Eine vollständige Versicherung der Gesamtrisikoposition würde allerdings aufgrund von Kosten- und Nutzenabwägungen an der Höhe der Prämien scheitern. Auch im Bereich der operationelle Risiken bestehen mittlerweile Versicherungsprodukte[97], die auf deren Besonderheiten zugeschnitten sind (Piaz 2002, 144). Die Versicherbarkeit scheitert zudem vielfach an Kriterien, die seitens der Versicherer eingefordert werden. So ist die Versicherbarkeit nach Karten von mehreren Kriterien abhängig. Zum einen muss Zufälligkeit erfüllt sein, nach der das den Versicherungseintritt auslösende Ereignis zum Zeitpunkt des Vertragsabschlusses nicht bekannt und unbeeinflussbar ist. Zum anderen muss das Kriterium Eindeutigkeit erfüllt sein, nach dem der Eintritt des Schadens und dessen Höhe objektiv nachprüfbar sind, während Schätzbarkeit voraussetzt, dass eine Versicherungsgesellschaft die Verteilung der Eintrittswahrscheinlichkeit und Schadenshöhe schätzen kann. Die Erfüllung des Kriteriums Unabhängigkeit bezieht Interdependenzen ein und setzt den Ausschluss positiv korrelierter Risiken voraus, während das Kriterium Größe voraussetzt, dass ein von der Versicherung zu tragender Maximalschaden definiert wird (Karten 1972, 279ff).

Teilen: Bei interorganisationalen Arrangements, wie z.B. Kooperationen, Outsourcing- oder Lieferbeziehungen, stellt auch die Teilung von Risiken zwischen mehreren Partnern eine weitere Handlungsalternative dar. So können beispielsweise Investitionen gemeinsam getätigt werden oder Risiken durch vertragliche Vereinbarungen zwischen den Partnern aufgeteilt werden (Andersson, Norrman 2004, 162f; Norrman, Lindroth 2004, 22). Diese Handlungsalternative geht in eine ähnliche Richtung wie die Überwälzung, wird aber als eigenständig angesehen, da im Falle des Teilens das Interesse einen Schadenseintritt zu verhindern, vergleichsweise höher ist, als im Falle einer Versicherungslösung.

Akzeptieren: RM umfasst nicht nur das Ergreifen von Maßnahmen zur Reduktion von Risiken, sondern auch das bewusste Eingehen von Risiken nach entsprechender Abwägung der zur Verfügung stehenden Handlungsoptionen und des mit deren Ergreifen verbundenen Aufwands. Somit stellt auch das Akzeptieren eine Handlungsalternative dar, nach der Risiken bewusst selbst getragen und keine Anstrengungen unternommen werden, um das Risiko zu reduzieren oder auszuschließen. Ein derartiger Verzicht erfolgt insbesondere bei geringfügigen Risiken, weil das Ergreifen von Steuerungsmaßnahmen vielfach mit einem unverhältnismäßig hohen Aufwand verbunden ist. Zudem müssen Risiken

[97] Ein Beispiel stellt die Financial Institutions Operational Risk Insurance von Swiss Re dar.

akzeptiert werden, wenn sie durch Maßnahmen nicht eliminierbar sind. Dennoch ist eine permanente Überwachung dieser Risiken bedeutend, da auch die Kumulation akzeptierter und minimaler Risiken im Zeitverlauf zu existenziellen Risiken führen kann (Hornung et al. 1999, 321; Junginger, Krcmar 2003, 20; Diederichs et al. 2004, 193; Williams et al. 2006, 71). Zudem setzt diese Alternative ein ausreichend vorhandenes Risikodeckungspotential voraus (Wyss 2000, 179f; Einhaus 2002, 490).

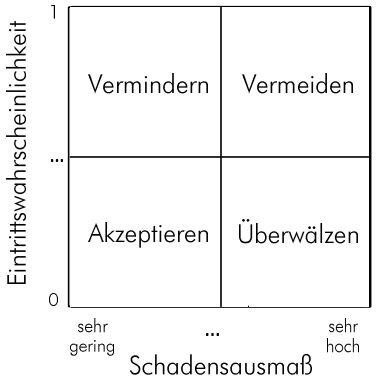


Abb. 16 Handlungsalternativen im Risiko-Portfolio[98]

Im Hinblick auf das zuvor dargestellte Risiko-Portfolio (siehe Abb. 13 auf Seite 81) können die verschiedenen Handlungsalternativen entsprechend der Dimensionen Eintrittswahrscheinlichkeit und Schadensausmaß wie in Abb. 16 dargestellt zugeordnet werden (Piaz 2002, 144). Dabei ist diese Einordnung allerdings nicht als vollkommen trennscharf zu verstehen, da z.B. Versicherungslösungen auch für Risiken, die ein geringes Schadensausmaß und eine hohe Eintrittswahrscheinlichkeit aufweisen, bestehen können oder bestimmte Risiken mit einem hohen Schadensausmaß mangels anderer Handlungsalternativen akzeptiert werden müssen.

Im Idealfall stehen zur Bewältigung der Einzelrisiken bzw. der Risikogruppen mehrere Steuerungsmaßnahmen, die zu deren Reduktion eingesetzt werden können, zur Auswahl. Die Auswahlentscheidung wird allerdings durch eine Vielzahl an Faktoren bestimmt, die das Budget, die Dringlichkeit oder die Effektivität der Maßnahmen betreffen. Kontio (2001, 82) definiert zur Unterstützung dieser Auswahlentscheidung verschiedene Kriterien. So sollten zuerst diejenigen Risiken gesteuert werden, die im Risiko-Portfolio der höchsten Risikoklasse zugeordnet sind, da sie existenzielle Auswirkungen haben können. Danach können Risiken niedrigerer Risikoklassen gesteuert werden. Einen weiteren bei der Maßnahmenauswahl zu beachtenden Einflussfaktor stellt die Dringlichkeit der Risikosteuerung dar. Diese ist sowohl vom Eintrittszeitpunkt des Risikos als auch vom Zeitbedarf der Implementierung der Maßnahme abhängig. Somit wird bei Dringlichkeit die Implementierung zeitaufwändiger Maßnahmen ausgeschlossen und so die zur Verfügung stehenden Alternativen eingeschränkt. Auch die Präferenzen der Stakeholder und insbesondere Kunden sind bei der Auswahl der Steuerungsmaßnahmen zu beachten, da diese potentiell die Risiken anders einschätzen und somit eventuell auch das Ergreifen bestimmter Maßnahmen einfordern. Die Auswahlentscheidung wird zudem durch die verfügbaren Budgets eingeschränkt, die das Ergreifen bestimmter Maßnahmen aus Aufwandsgründen behindern können. Aufgrund knapper Budgets und der Forderung eines ökonomischen Einsatzes der Steuerungsmaßnahmen stellt auch deren Effizienz ein Auswahlkriterium dar, dem besondere Bedeutung beizumessen ist.

[98] In Anlehnung an (Piaz 2002, 144).

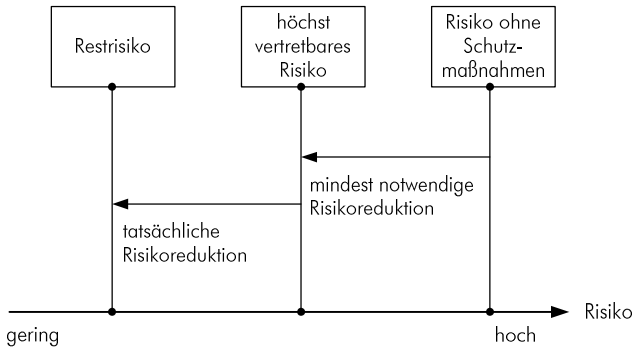


Abb. 17 Abgrenzung des Restrisikos[99]

Abschließend zur Steuerung soll noch deren Ergebnis anhand Abb. 17 erläutert werden. Ausgehend von der Situation, dass keine Steuerung erfolgt, ist das Gesamtrisiko am höchsten. In Abhängigkeit der individuellen Risikobereitschaft und des Risikodeckungspotentials des Unternehmens werden Steuerungsmaßnahmen ergriffen, um das Risiko zu begrenzen. Dabei sind einige Maßnahmen erforderlich, um Risiken auf ein höchst vertretbares Niveau zu reduzieren. Dies kann z.B. die Steuerung von bestandsgefährdenden Risiken nach KonTraG (siehe 3.6) betreffen. Über dieses Niveau hinausgehend werden Maßnahmen ergriffen, die zur Folge haben, dass ein der Risikoneigung und dem Risikodeckungspotential entsprechendes Restrisiko[100] verbleibt, das bewusst akzeptiert oder nicht vermeidbar ist (KPMG 1998, 17; Seibold 2006, 25).

3.5.5 Risikoüberwachung

Im Rahmen der Risikoüberwachung werden die risikopolitischen Entscheidungen auf ihre Wirksamkeit und ihren ökonomischen Nutzen überprüft (Schulte 1997, 17). Dabei kann zwischen einer Überwachung der Steuerung und einer Gesamtprozessüberwachung unterschieden werden. Erstere dient zur Kontrolle des Effektes der Steuerungsmaßnahmen und den mit ihnen verbundenen Zielen, während die Gesamtkontrolle sämtliche Phasen des RM-Prozesses einer näheren Betrachtung unterzieht. Neben der Effektivität stellt auch die organisatorische Umsetzung einen Prüfgegenstand dar. So wird im Hinblick auf die Risikoidentifikation deren Vollständigkeit überprüft und bzgl. der Risikobewertung ein Abgleich der Prognosewerte zu Eintrittswahrscheinlichkeiten und Schadensausmaßen mit den tatsächlichen Werten vorgenommen (Henselmann 2001, 40; Einhaus 2002, 490; Prokein 2005, 9). Im Hinblick auf die Steuerung wird die Wirksamkeit der ergriffenen Maßnahmen laufend überprüft. Das allgemeine Ziel dieser Prozessphase besteht darin, die permanente Überwachung der Risikosituation und die Funktionsfähigkeit der Maßnahmen sicherzustellen, wobei die Kontrollen prozessbezogen, prozessübergreifend oder prozessunabhängig sein können. Die Kontrollen werden gegenüber den operativ Risikoverantwortlichen ausgeübt, die mit der Ausführung der jeweiligen Aufgaben beauftragt sind. Dabei kann auch durch eine Funktionstrennung gewährleistet werden, dass sowohl auf operativen als auch auf strategischen Managementebenen diejenigen Entscheidungen überwacht werden, die

[99] In Anlehnung an http://www.schaffar.com/risikoqu.htm.

[100] Als Restrisiko wird die Gefährdung bezeichnet, die einer Tätigkeit, einer Methode, einem Verfahren oder einem Prozess nach dem Stand der Wissenschaft selbst bei Anwendung aller theoretisch möglichen Sicherheitsvorkehrungen noch anhaftet. (aus Münchner Rück: http://www.munichre.com/).

potentiell zu einem Risiko führen (Hornung et al. 1999, 321; PWC 2001, 20). In Abhängigkeit der Erkenntnisse zur Effektivität der Methoden und Maßnahmen sowie deren organisatorischer Umsetzung kann eine Anpassung der Risikostrategie im Allgemeinen und der konkreten Ausgestaltung der einzelnen Phasen des RM-Prozesses erfolgen (Wall 2001, 214).

Nachdem die Phasen des RM-Prozesses durchlaufen wurden, kann der Prozess auch um Aufgaben im Bereich der Risikofrüherkennung erweitert werden (Reh 2001, 33). Die frühzeitige Erkennung von Risiken wird auch im Rahmen des KonTraG (siehe 3.6.1) gefordert und kann durch den gezielten Einsatz von Indikatoren erfolgen. Dabei weichen die Interpretationen zum Gegenstand der Früherkennung weit voneinander ab, wobei Risikofrüherkennungssysteme, als fortgeschrittene auf Indikatoren basierende Systeme, noch nicht umfassend in Unternehmen eingesetzt werden (Hahn, Krystek 2000, 75; Wall 2001, 220; Tewald 2004, 262). Indikatoren können allgemein in Früh- und Spätindikatoren unterschieden werden, wobei erstere auf zukünftige Risikoereignisse hinweisen und Spätindikatoren bereits eingetretene Risikoereignisse reflektieren (Romeike 2004a, 48). Erstere beziehen sich auf einen oder mehrere Geschäftsprozesse und können herangezogen werden, um Veränderungen der Risikosituation zu erkennen. Sie sollten dabei eine verlässliche Basis für die Vorhersage der Entwicklung von Eintrittswahrscheinlichkeit und Schadensausmaß des Risikos darstellen. Auf diese Weise kann der Realisierung von Fehlentwicklungen bzw. Risiken frühzeitig entgegengewirkt werden[101]. Da Indikatoren auch falsche Aussagen liefern können, ist auf deren Auswahl besonderer Wert zu legen (DeMarco, Lister 2003, 72f). Daher sollten Indikatoren eng mit dem Risiko in Bezug stehen, quantifizierbar, einfach beobachtbar und gut dokumentiert sein, um richtige Prognosen zu liefern und effizient eingesetzt werden zu können (Romeike 2004a, 48; Scandizzo 2005, 239). Risikoindikatoren werden im Rahmen der Risikoüberwachung laufend mit einer Sollgröße verglichen. Wird eine definierter Schwellenwert überschritten, so erfolgt eine Meldung an die Risikoverantwortlichen, um zeitnah Gegenmaßnahmen einleiten zu können (Klomfass, Quadt 2001, 325f; van den Brink 2001, 39f). Während der Einsatz von Indikatoren zur Früherkennung im Bereich der finanziellen Risiken seit langem verbreitet ist, steht deren Entwicklung im Falle operationeller Risiken noch am Anfang (Locher 2004, 33).

3.5.6 Risikokommunikation und -dokumentation

Neben der Risikostrategie und den Kernaufgaben tragen insbesondere auch die unterstützenden Aufgaben Risikokommunikation und -dokumentation zur leistungsfähigen Umsetzung des RM bei. Durch die Risikokommunikation wird sichergestellt, dass alle Mitarbeiter über die Risikostrategie und die

[101] Indikatoren können verschiedenen Quellen entstammen und sich z.B. auf Kennzahlen im Bereich Personal (z.B. Fluktuations- und Krankheitsquoten), die eingesetzten Systeme (z.B. Systemausfallzeiten, Sicherheitsvorfälle) oder Prozesse (z.B. Fehlerquote pro Arbeitsschritt) beziehen (Klomfass, Quadt 2001, 7*; van den Brink 2001, 39; Basel 2003, 8; Kütz 2003, 147ff; Oepping, Siemes 2003, 232; Schmitting, Siemes 2004, 105; Scandizzo 2005, 235).

korrespondierenden Anforderungen informiert sind sowie Risikobewusstsein geschaffen wird (Wallmüller 2004, 3). Von dieser internen Fokussierung kann die externe Risikokommunikation abgegrenzt werden, die Anlegern und sonstigen Dritten Informationen unterschiedlicher Art zur Verfügung stellt (PWC 2001, 20f; Mosiek 2003, 15ff). In diesem Kontext ist es zentral, dass die Entscheidungsträger über aktuelle Risiken informiert sind, um Steuerungsmaßnahmen einleiten zu können. Dabei kommt v.a. auch der Definition von Wesentlichkeitsgrenzen, durch die geregelt wird, wann die Behandlung eines Risikos an die nächste Berichtsebene eskaliert wird, eine besondere Bedeutung zu (Kuhn 2002, 16; von Hohnhorst 2002, 100). Zur Berichterstattung kann ein Risikoportfolio (siehe auch Abb. 13 auf Seite 81) herangezogen werden, in das die Risiken anhand der Dimensionen Eintrittswahrscheinlichkeit und Schadensausmaß eingeordnet werden und das sich als branchenübergreifender Standard herausgestellt hat. Entsprechend der Einordnung werden diejenigen Risiken, die die definierte Wesentlichkeitsgrenze übersteigen, berichtet (Wolf 2004, 215). Zudem ist die Berichterstattung über nicht bewältigte Risiken und eine Weiterleitung der Informationen an eine entsprechende Stelle erforderlich (IDW 1999, Tz 11).

Risikokommunikation stellt die Grundlage eines wirksamen RM dar und kann nach Erdenberger an die Qualitätsmanagement-Arbeitskreise nach ISO 9000ff angelehnt werden. Somit erfolgt eine regelmäßige Berichterstattung zu den Risiken, den eingeleiteten und zukünftigen Maßnahmen des Unternehmensbereiches, um so das Risikobewusstsein zu erhöhen (Erdenberger 2001, 15).

Ebenso wie die Risikokommunikation unterstützt auch die RM-Dokumentation die Durchführung der Kernaufgaben und kann zudem als Nachweis über pflichtgemäßes Verhalten, das im Rahmen der Regulation (z.B. KonTraG) eingefordert wird, dienen (PWC 2001, 20f; Junginger, Krcmar 2003, 21)[102]. Dabei sollte die RM-Dokumentation als Mindestinhalte gesetzliche Grundlagen, Risikodefinition, risikopolitische Grundsätze, Ziele und Aufgaben des RM, Erläuterungen zum Aufbau und Ablauf der RM-Organisation, Dokumentation und Erläuterung des Instrumentariums zur Unterstützung der Kernaufgaben, Verhaltensregeln zum Einsatz des Instrumentariums, Verhaltensregeln zur Risikokommunikation sowie eine Dokumentation des Revisionsprozesses umfassen (Diederichs et al. 2004, 196f). Die RM-Dokumentation kann dabei mittels eines RM-Handbuches systematisiert werden (PWC 2001, 21).

Die effiziente Umsetzung des RM kann über die verschiedenen Prozessphasen hinweg ein Risikoinventar (siehe Abb. 12) zugrunde legen, das sukzessive in Abhängigkeit des Status der Risiken angepasst wird. So können im Rahmen der Risikoidentifikation die identifizierten Risiken anhand verschiedener Kategorien wie Risikokategorie, Unternehmensbereich, Wirkung, Zeitbezug, Realisierungsgrad, Bewältigung, Relevanz sowie Qualität der Erfassung systematisiert werden (Schulte 1997,

[102] So wird im Rahmen des KonTraG nach § 289 HGB eine umfassende Berichterstattung über Risiken sowie deren zukünftige Entwicklung im Lagebericht gefordert (siehe hierzu auch Abschnitt 3.6).

15; Happel, Liebewein 2000, 5; Gleißner 2001, 113; Mott 2001, 204; Aubert et al. 2002, 157; Mosiek 2003, 16). Dabei kann die jeweilige Risikokategorie (z.B. leistungswirtschaftliches oder finanzielles Risiko) angegeben werden, die sich an der zugrunde gelegte Kategorisierung von Risiken (siehe Abb. 10 Seite 68) anlehnen kann (Schulte 1997, 15; Mott 2001, 205).

Eine weitere Spezifizierung z.B. im Hinblick auf die Verantwortlichkeit kann durch die Angabe des Unternehmensbereiches (z.B. Vertrieb, Produktion) erreicht werden (Happel, Liebewein 2000, 4f). Als generisch für Industrieunternehmen erweist sich in diesem Kontext die Gliederung der Unternehmensbereiche nach den Primäraktivitäten Eingangslogistik, Produktion, Ausgangslogistik, Marketing und Verkauf sowie Kundendienst und den Sekundäraktivitäten der Wertschöpfungskette, unter die Unternehmensinfrastruktur, Personalwirtschaft, Technologieentwicklung und Beschaffung subsumiert werden (Porter 1985, 36ff). Die Wirkung des Risikos kann im Rahmen der Risikoidentifikation grob bestimmt werden. So kann generell eine monetäre, qualitative und reputationsbezogene Wirkung unterschieden werden. Darüber hinaus kann hinsichtlich des Zeitbezugs das Risiko als kurz-, mittel- oder langfristig spezifiziert werden und auch der Realisierungsgrad, der die Ausprägungen bestehend oder möglicherweise entstehend annehmen kann, angegeben werden (Happel, Liebewein 2000, 4f; Klomfass, Quadt 2001, 322ff; Mott 2001, 205). Da der Zuweisung von klaren Verantwortlichkeiten im RM eine besondere Bedeutung zukommt, sollte ein Risikoverantwortlicher bzw. eine entsprechende Organisationseinheit angegeben werden. Bei Änderungen ist eine entsprechende Anpassung vorzunehmen. Ferner kann die Durchführung der Aufgaben in den nachfolgenden Prozessphasen durch die Angabe von Vorschlägen zu Bewältigungsmaßnahmen sowie eine grobe Einschätzung der Relevanz des Risikos unterstützt werden (Gleißner 2001, 113). Zudem kann die Qualität der Risikoidentifikation, die von gering bis sehr präzise reichen kann, angegeben werden, um so den Handlungsbedarf in den nachfolgenden Prozessphasen transparenter zu machen (Mott 2001, 205).

Im Rahmen der Risikobewertung kann das Risikoinventar um verschiedene Aspekte erweitert werden. So werden in diesem Prozessschritt primär die Höhe des Schadens sowie dessen Eintrittswahrscheinlichkeit ermittelt. Der sich daraus ergebende Wert, der den potentiellen Schaden angibt, kann auch als Bruttorisiko bezeichnet werden. Aus diesen Größen lässt sich zudem in Abhängigkeit der unternehmensindividuellen Risikoneigung die Risikoklasse ermitteln, die einen bestimmten Handlungsbedarf für die Risikosteuerung nach sich zieht (Erdenberger 2001, 15; Geiger, Piaz 2001, 797; Thomson 2005, 133). Wenn nicht bereits im Rahmen der Risikoidentifikation ein Risikoverantwortlicher bestimmt wurde, so ist dies spätestens in dieser Phase erforderlich. Dabei können sich Verantwortlichkeiten auch im Zeitablauf ändern, was in diesem Fall auch zu vermerken ist (Erdenberger 2001, 15; Mott 2001, 204). Zudem können Frühwarnindikatoren für Risiken in das Risikoinventar einbezogen werden. Frühwarnindikatoren, wie z.B. schlechte Arbeitsmoral, sind insbesondere im Bereich der operationellen Risiken relevant, da diese vielfach nicht direkt erkennbar sind (Piaz 2002, 80). Potentielle

Frühwarnindikatoren können dabei aus der Anwendung der verschiedenen Bewertungsmethoden zur detaillierten Betrachtung von Risiken gewonnen werden, wobei insbesondere Indikator-Ansätze und Kausal-Methoden zu deren Identifikation geeignet sind.

Element des Risikoinventars	Ausprägung				
Risikokategorie	leistungs-wirtschaftlich	finanziell	Management / Organisation	extern	
Unternehmensbereich (Primäraktivität)	Eingangs-logistik	Produktion	Ausgangs-logistik	Marketing und Verkauf	Kunden-dienst
Unternehmensbereich (Sekundäraktivität)	Unternehmens-infrastruktur	Personal-wirtschaft	Technologie-entwicklung	Beschaffung	
Wirkung	monetär	qualitativ	reputationsbezogen		
Zeitbezug	kurzfristig	mittelfristig	langfristig		
Realisierungsgrad	bestehend	potenziell entstehend			
Qualität der Erfassung	sehr gering	gering	mittel	hoch	sehr hoch
Eintritts-wahrscheinlichkeit	sehr gering	gering	mittel	hoch	sehr hoch
Schadensausmaß	sehr gering	gering	mittel	hoch	sehr hoch
Bruttorisiko					
Risikoklasse / Erwartungswert	vernach-lässigbar	tragbar	vertretbar	nicht annehmbar	
Risiko-verantwortlicher					
ergriffene Maßnahmen					
Nettorisiko					
zuk. Maßnahmen / Vorschläge					
Frühwarnindikatoren					

Tab. 4 Risikoinventar

Im Rahmen der Risikosteuerung kann das Risikoinventar um die durchgeführten Aktionen erweitert werden. So kann je identifiziertem und bewertetem Risiko bzw. Risikogruppe zusätzlich angegeben werden, welche Maßnahmen ergriffen wurden, um das Risiko zu reduzieren (Erdenberger 2001, 15; Geiger, Piaz 2001, 797; Gleißner 2001, 113; Thomson 2005, 133). Potentiell veränderte Verantwortlichkeiten, die sich beispielsweise aus einer Eskalation des Risikos ergeben, sind ebenfalls zu vermerken. Zudem können die Effekte der Steuerungsmaßnahmen, soweit dies im Rahmen dieser Phase möglich ist, angegeben werden. Ausgehend vom Bruttorisiko, das das Schadensausmaß bezeichnet, das sich bei Eintritt des Schadens ohne Einleitung von Steuerungsmaßnahmen ergeben würde, kann das Nettorisiko als potentiell verbleibender Restschaden bei Einleitung der Steuerungsmaßnahmen, angegeben werden. Zusätzlich können Maßnahmen angegeben werden, die im zukünftigen Umgang mit dem Risiko bzw. der Risikogruppe erforderlich sind (Erdenberger 2001, 15). Diese Erweiterungen des Risikoinventars sind in Tab. 4 visualisiert.

3.6 Vorschriften zum Risikomanagement

Hinsichtlich RM bestehen eine Reihe verschiedener Vorschriften seitens des Gesetzgebers oder von Seiten spezifischer Institutionen. Im Rahmen dieses Abschnittes werden als weit verbreitete Vorschriften das KonTraG (siehe 3.6.1), das Kapitalgesellschaften in Deutschland betrifft, Basel II (siehe 3.6.2), durch das internationale Banken weltweit reguliert werden sowie der Sarbanes-Oxley-Act (siehe 3.6.3), der an der US-Börse gelistete Unternehmen betrifft, näher betrachtet.

3.6.1 KonTraG

Das 1998 verabschiedete KonTraG hebt explizit die Sorgfaltspflicht börsennotierter Aktiengesellschaften in Bezug auf Risiko hervor (1998), um die Interessen der Anteilseigner zu wahren (Lück 1998, 8ff). Das KonTraG selbst ist nicht als ein eigenständiges Gesetz zu betrachten, sondern als ein Konstrukt aus zahlreichen Änderungen und Ergänzungen im Aktiengesetz (AktG) und Handelsgesetzbuch (HGB) (Keitsch 2000, 14).

Das KonTraG wird in der Literatur vielfach auf RM reduziert, obwohl die Intention des Gesetzgebers weiter gefasst ist. So sind im KonTraG die Verbesserung der Transparenz für die Anteilseigner, die Stärkung der Kontrolle durch die Hauptversammlung und somit insgesamt eine Verbesserung der Corporate Governance vordergründig (Bitz 2000, 4; Picot 2001, 8; von Hohnhorst 2002, 93; Wallmüller 2004, 3). Hinsichtlich RM besteht der Kern des Gesetzes darin, dass die Haftung von Vorstand, Aufsichtsrat und Wirtschaftsprüfer erweitert wird und die Unternehmensleitung ein unternehmensweites Früherkennungssystem für Risiken einzurichten hat sowie Risiken, Risikostruktur und deren Entwicklung im Lagebericht (§ 289 HGB) des Jahresabschlusses[103] zu veröffentlichen sind. So wird in § 91 AktG der Vorstand der Aktiengesellschaft verpflichtet, für ein angemessenes RM zu sorgen sowie dazu „geeignete Maßnahmen zu treffen, insbesondere ein internes Überwachungssystem[104] einzurichten“. Das Gesetz gibt allerdings keinen Aufschluss darüber, wie das RM im Detail auszugestalten ist, sondern verweist nur darauf, dass sich der Vorstand bei der Ausgestaltung an der gebotenen Sorgfalt eines ordentlichen und gewissenhaften Geschäftsführers zu orientieren hat (§ 93 AktG).

Das KonTraG mit seinem ausdrücklichen Gebot eines Risikoüberwachungssystems betrifft nur Aktiengesellschaften und Kommanditgesellschaften auf Aktien (KGaA). Jedoch spricht der Gesetzgeber die Erwartung aus, dass das Gesetz eine Ausstrahlungswirkung auf andere Rechtsformen, insbesondere die GmbH hat (§ 43 GmbHG), obwohl im GmbHG keine eigenständigen Regelungen getroffen sind.

Das KonTraG fokussiert Risiken, die mit einer Bestands- bzw. Existenzgefährdung verbunden sind. Der Begriff ist unscharf und kann unterschiedlich weit ausgelegt werden. Wambach empfiehlt eine derartige weite Auslegung und fasst darunter alle Risiken, die sich direkt oder indirekt auf die Vermögens-, Ertrags-, und Finanzlage des Unternehmens auswirken und dessen Existenz gefährden (Wambach 2002, 216). Eine Erweiterung der Betrachtung auf nicht bestandsgefährdende Risiken ist zudem sinnvoll, da einerseits Risiken in ihrer Aggregation eine Bestandsgefährdung auslösen können und andererseits eine Bestandsgefährdung oftmals nicht oder nur schwer erkennbar ist.

[103] Im Falle von Konzernen erfolgt die Angabe im Konzernlagebericht des Konzernabschlusses § 315 I HGB.

[104] Zur Überwachung im Unternehmen bestehen verschiedene Möglichkeiten, wie Überwachung durch ein internes Überwachungssystem, Überwachung durch den Abschlussprüfer, Überwachung durch den Aufsichtsrat sowie Überwachung im Rahmen der Konzernüberwachung (Rockel 2002, 7ff).

Bei der Abschlussprüfung wird durch den Wirtschaftsprüfer beurteilt, ob (gem. § 317 IV HGB) der Vorstand den entsprechenden Pflichten nachgekommen ist. Demzufolge besteht seitens der Wirtschaftsprüfung in der Form eines spezifischen Prüfstandards (IDW PS 340) eine über den Gesetzestext hinausgehende Konkretisierung der Ausgestaltung eines KonTraG-konformen RM nach § 91 II AktG. Demnach sind durch die Unternehmensleitung auf der Basis definierter Risikofelder Risiken zu erfassen (IDW 1999, Tz 7-8). Diese Risiken sind im Hinblick auf Eintrittswahrscheinlichkeit und Schadensausmaß zu bewerten sowie zu einer Gesamtrisikoposition zu aggregieren. Zudem soll Risikobewusstsein bei den Mitarbeitern geschaffen werden (IDW 1999, Tz 9-10). Darüber hinaus ist eine umfassende Risikokommunikation im Unternehmen zu implementieren, die neben einer Schulung der Kommunikationsbereitschaft auch Schwellenwerte für entsprechende Berichtspflichten, definierte Überwachungszyklen und eine nachweisbare Berichterstattung über nicht bewältigte Risiken umfasst (IDW 1999, Tz 11-12). Zudem sind organisatorische Verantwortlichkeiten verschiedener Managementebenen sowie entsprechende Eskalationsprozesse bei Nichtbewältigung der Risiken nachweisbar zu implementieren (IDW 1999, Tz 13-14). Ferner ist ein Überwachungssystem einzurichten, mittels dessen die Wirksamkeit der ergriffenen Maßnahmen und der Kommunikation kontrolliert wird. Dies kann auch Gegenstand der internen Revision sein (IDW 1999, Tz 15-16). Das Überwachungssystem hat dabei eine Präventiv- und eine Korrekturfunktion. Erstere dient zur Reduktion der bestehenden bzw. potentiellen Risiken, während mittels Korrekturfunktion die Wirksamkeit der Maßnahmen überprüft wird und gegebenenfalls Anpassungen vorgenommen werden (Lück et al. 2002, 231). Zudem sind im Rahmen der Risikodokumentation Nachweise im Hinblick auf die im RM ergriffenen Aktivitäten zu erbringen und ein Risikohandbuch zu erstellen (IDW 1999, Tz 17-18). Die aus dem KonTraG erwachsenden Pflichten im Hinblick auf die Implementierung eines leistungsfähigen RM sind somit entsprechend konkretisierbar und stellen bei Kapitalgesellschaften einen Prüfgegenstand im Rahmen der Abschlussprüfung dar.

3.6.2 Basel II

Hohe Insolvenzraten, Kreditausfälle und volatile Märkte haben zur Folge, dass Unternehmen der Finanzwirtschaft umfassend von aufsichtsrechtlichen Regulierungen betroffen sind. Demnach müssen Kreditinstitute ihre Bankgeschäfte mit Eigenkapital hinterlegen, was zum einen der Stabilität der Finanzwirtschaft und zum anderen dem Schutz der Gläubiger dient (Locher et al. 2004, 15ff). Mit dem Ziel, die Eigenkapitalvorschriften international zu vereinheitlichen, wurde 1974 der Baseler Ausschuss für Bankenaufsicht von den G-10 Staaten mit Sitz in Basel gegründet[105]. Nach der Veröffentlichung 1988 trat 1992 der Baseler Eigenkapitalakkord (Basel I), nach dem Kreditgeschäfte mit Eigenkapital zu unterlegen sind, in Kraft. Bedingt durch die Ausweitung der Derivat- und Handelsgeschäfte

[105] Der Baseler Ausschuss arbeitet unter dem Dach der Bank für internationalen Zahlungsausgleich (BIZ) in Basel.

der Banken erfolgte 1996 eine Erweiterung auf Marktrisiken, die es von nun an ebenfalls mit einem ermittelten Prozentsatz an Eigenkapital zu hinterlegen galt. Dieser Teil des Eigenkapitals wird auch als regulatorisches Eigenkapital bezeichnet. Seit Einführung der ersten Eigenkapitalvereinbarung 1992 erfolgte eine Umsetzung in einem Großteil der Länder, in denen internationale Banken tätig sind, was auf den hohen Stellenwert hinweist (Locher et al. 2004, 19f; Hofmann 2006, 93).

Bedingt durch die Weiterentwicklung der Bewertungsmethoden der Risiken sowie das Auftreten von Krisen bzw. Zusammenbrüche verschiedener Banken (z.B. Barings Bank[106]) wurde 1999 in der Form eines Konsultationspapiers, dem in den folgenden Jahren zwei weitere folgten, mit der Entwicklung des neuen Baseler Eigenkapitalakkords (Basel II) begonnen, der nunmehr neben einer Überarbeitung von Basel I auch operationelle Risiken in die Risikobetrachtungen bzw. in die Eigenkapitalhinterlegung einbeziehen sollte (Hofmann 2006, 94). Seit 1. Januar 2007 sind die Regelungen nach Basel II verbindlich in den Mitgliedsstaaten der Europäischen Union nach der EU-Richtlinie 2006/49/EG anzuwenden, wobei eine einjährige Übergangsfrist besteht. Die Umsetzung dieser Mindesteigenkapitalanforderungen erfolgt im deutschen Recht mittels der Solvabilitätsverordnung (SolvV).

Um die Höhe des regulatorischen Eigenkapitals zu bestimmen, werden im Rahmen von Basel II drei verschiedene Verfahren zur Bewertung operationeller Risiken zur Auswahl gestellt (Basel 2004, 157ff). Der Basisindikatoransatz bezieht sich auf einen einzelnen Indikator α (15%), der mit dem Dreijahresdurchschnitt des Bruttoertrages multipliziert das zu unterlegende Eigenkapital bestimmt (siehe auch § 270 SolvV). Im Rahmen des Standardansatzes werden die jeweiligen Bruttoerträgen der acht verschiedenen Geschäftsfelder einer Bank mit einem festen β-Faktor[107] multipliziert und dann zu einem so genannten Teilanrechnungsbetrag aufsummiert. Diese Beträge werden für die letzten drei Jahre ermittelt, wobei sich die Eigenkapitalunterlegung aus deren Mittelwert ergibt (siehe auch § 272ff SolvV).

Als dritte Möglichkeit können fortgeschrittene Messansätze zur Ermittlung des zu hinterlegenden Eigenkapitals herangezogen werden, wobei für diese im Gegensatz zu den beiden zuvor genannten Verfahren keine festen Vorgaben zur Ermittlung bestehen. Zur Ermittlung der Eigenkapitalhinterlegung können beispielsweise ein interner Bemessungs-, ein Verlustverteilungs- oder ein Scorcard-Ansatz herangezogen werden, sofern Verlustdaten der letzten fünf Jahre vorliegen. Für die Anwendung fortgeschrittener Messansätze müssen allerdings eine Reihe von Anforderungen (§§ 279-292 SolvV) vollständig erfüllt sein. Je nach Wahl des Bewertungsansatzes sind unterschiedliche qualitative Anforderungen zu erfüllen, die sowohl in der Solvabilitätsverordnung als auch in den so genannten Sound Practices geregelt sind, wobei die Anforderungen bei der Verwendung des Basisindikatoransatzes geringer sind und insbesondere bei fortgeschrittenen Messansätzen deren Erfüllung unerlässlich ist

[106] Die Barings Bank erlitt 1995 durch nicht autorisierte Zins- und Währungsspekulationen eines Wertpapierhändlers in Asien einen Verlust von 1,4 Milliarden US-Dollar, was zur Insolvenz der Barings Plc. führte.

[107] Diese sind in § 272 IV SolvV bestimmt und liegen zwischen 12 und 18 %.

(Hauri, Lecomte 2007, 171). In den Sound Practices, in denen Angaben zu Rahmenbedingungen, Kernaufgaben, Rolle der Bankaufsicht und Offenlegung gemacht werden, erfährt das RM eine weitere Konkretisierung[108].

3.6.3 Sarbanes-Oxley Act

2002 trat als Reaktion auf verschiedene Finanzskandale von U.S. Unternehmen (z.B. Enron) der Sarbanes-Oxley-Act (SOX) in Kraft, der wie auch das KonTraG ein Artikelgesetz darstellt. Gegenstand dieses Gesetzes sind die Einhaltung der Corporate Governance von an U.S. Börsen notierten Unternehmen sowie Regulierungsmaßnahmen für die amerikanischen Wirtschaftsprüfer. Dabei hat das Gesetz auch Auswirkungen auf das RM im Unternehmen. Der SOX ist auch für deutsche Unternehmen gültig, wenn deren Anteile an der U.S. Börse gelistet sind oder die Wertpapiere auf anderen Wegen öffentlich in den USA anbieten (Locher 2004, 21; Menzies 2004, 13). Das zentrale Ziel des SOX ist, das Vertrauen der Anleger durch die Verbesserung der Transparenz von Unternehmensprozessen und die gezielte Information der Adressaten der Finanzberichterstattung sicherzustellen.

Der Sarbanes-Oxley Act ist in elf Sektionen gegliedert, die sich beispielsweise mit der Unabhängigkeit der Wirtschaftsprüfer (Sektion 2), den Verantwortlichkeiten im Unternehmen (Sektion 3) oder der Veröffentlichung von Finanzdaten (Sektion 4) befassen, wobei der Kern des Gesetzes die Verpflichtung zur Richtigkeit der Finanzzahlen darstellt. Dazu wird im Falle der Aktiengesellschaft durch den Vorstandsvorsitzenden und den Finanzvorstand jährlich und öffentlich an Eides statt erklärt, dass die Finanzzahlen des Unternehmens auf wahren Tatsachen beruhen und die wirtschaftliche Lage widerspiegeln. Voraussetzung der Erklärung dieser Zahlen ist die Einrichtung eines internen Kontrollsystems. Falschangaben werden mit hohen persönlichen Strafen geahndet, wie Geldstrafen bis zu 5 Mio. $ und Freiheitsstrafen bis zu 20 Jahren (Lanfermann, Maul 2002, 1730; Locher 2004, 21; Brown, Nasuti 2005, 16).

Hinsichtlich RM ist dabei insbesondere das interne Kontrollsystem relevant, wobei die Sektionen 302 und 404 neben dem reinen Betrieb des Kontrollsystems auch eine Überprüfung dessen Wirksamkeit erfolgen muss, die auch vom Abschlussprüfer bestätigt werden muss. So ist die Veröffentlichung der Geschäftsberichte durch entsprechende Kontrollen zu flankieren, die regeln, welche rechnungslegungsrelevanten Informationen dem Management zugänglich gemacht werden sollen, wobei Kontrollen die Zuverlässigkeit der eingesetzten Systeme sicherstellen sollen. Im Rahmen von Sektion 404 ist nachzuweisen, dass Kontrollen zur Rechnungslegung implementiert wurden und über Unregelmäßigkeiten oder Schwachstellen Bericht erstattet wurde. Dabei ist die Überprüfung der Berichte des Managements zur Qualität der Kontrollen auch Prüfgegenstand.

[108] Siehe hierzu (Basel 2003).

3.7 Zusammenfassung und Diskussion

Im Rahmen dieses Kapitels wurden ausgehend von unterschiedlichen betriebswirtschaftlichen Perspektiven auf den Risikobegriff unterschiedliche Risikotypen erläutert, die für ein gezieltes RM von Relevanz sind. Für den vorliegenden Untersuchungsgegenstand ist von diesen insbesondere operationelles Risiko bedeutend, da dieser Risikotyp auf die Ebene der Geschäftsprozesse fokussiert ist und somit die Risiken den täglichen Aufgaben entspringen. Derartige Parallelen können auch auf den Wissensrisikobegriff übertragen werden, der in Abschnitt 5.1 erläutert wird. Ferner wurden in diesem Kapitel zum einen eine allgemeine Kategorisierung zu Risiken, die einen Standard darstellt, und eine Kategorisierung zu operationellen Risiken vorgestellt, um die Bandbreite der Risiken aufzuzeigen. Den Kern dieses Kapitels bilden der RM-Prozess und insbesondere die Kernaufgaben Identifikation, Bewertung, Steuerung und Überwachung, die durch eine Risikostrategie determiniert werden, die auf die Unternehmensziele ausgerichtet ist und die Risikobereitschaft des Unternehmens widerspiegelt.
Der RM-Prozess ist als permanenter Prozess zu verstehen, der durchgängig durch die entsprechende Führung eines Risikoinventars unterstützt werden kann. Dabei werden in der Praxis nicht alle Elemente zur Detaillierung der Aktivitäten im Umgang mit den Risiken umgesetzt, sondern dienen vielmehr als Gedankenstütze (Erdenberger 2001, 15). Jedoch dient eine umfassende Risikodokumentation z.B. in der Form eines solchen Risikoinventars als Nachweis darüber, dass die Geschäftsführung aktiv und ordentlich mit Risiken umgegangen ist und somit ihren Sorgfaltspflichten nachgekommen ist (PWC 2001, 20f). Somit leistet das Risikoinventar auch einen Beitrag zur Erfüllung der verschiedenen Regularien.
Die Kern- und Unterstützungsaufgaben können durch RM-Systeme unterstützt werden, die sicherstellen, dass in regelmäßigen Abständen die Risikosituation neu bewertet wird, die Ergebnisse der Unternehmensführung kommuniziert und rechtzeitig adäquate Risikobewältigungsmaßnahmen eingeleitet werden (Gleißner 2001, 111). Im Kontext von IT-Systemen stellen RM-Informationssysteme spezielle Werkzeuge zur Entscheidungsunterstützung dar. Sie unterstützen den RM-Prozess beispielsweise durch Simulationen, Schadensadministration, Risikokostenanalyse sowie durch die Erstellung entsprechender Reports (Erben, Romeike 2002, 561ff; Diederichs, Kaminski 2003, 699ff; Gleißner, Romeike 2005, 257).

4 IT-Risiko und IT-Risikomanagement

Im unternehmensweiten RM wird eine aggregierte Betrachtung von Risiken verschiedener Unternehmensbereiche vorgenommen. In Abhängigkeit der Unternehmensphilosophie, Branche, Relevanz von Vorschriften und organisatorischer Verankerung des RM bestehen unterschiedliche Schwerpunktsetzungen und Verantwortlichkeiten bei dessen Umsetzung. Dabei bestehen verschiedene Risikokategorien, die in den entsprechenden Fachbereichen analysiert und bei dezentraler Verantwortlichkeit auch gesteuert werden. So werden im finanzwirtschaftlichen Bereich Kredit- und Marktrisiken (z.B. Zinsrisiken) analysiert, im Ein- und Verkauf leistungswirtschaftliche Risiken (z.B. Absatzrisiken) oder in der Rechtsabteilung rechtliche Risiken (z.B. Produkthaftung). Risiken, die aus dem Einsatz der IT erwachsen, im Folgenden als IT-Risiken bezeichnet, stellen eine gesonderte Risikogruppe dar, die aufgrund der ausgeprägten Unterstützungsfunktion der IT nahezu alle Unternehmensbereiche betrifft. IT-Risiken stellen in diesem Zusammenhang eine Untergruppe der operationellen Risiken dar, was bedeutet, dass sie auch vorwiegend auf die Ebene der Geschäftsprozesse bezogen sind (Wolf 2005, 15)[109].

Dabei hat die Abhängigkeit von der IT seitens der Unternehmen im Allgemeinen und der Geschäftsprozesse im Speziellen in der Vergangenheit zugenommen, was dazu führt, dass die Risiken, die sich beispielsweise aus der mangelnden Verfügbarkeit der IT-Systeme ergeben, zugenommen haben (Noufal 2003, 141; Salmela 2003, 1; Suh, Han 2003, 149; Belsis et al. 2005, 189; Sitzberger, Nowey 2006, 159). Zudem hat in den vergangenen Jahren auch die Anzahl der Schadsoftware zugenommen, wobei insbesondere auch die Zusammensetzung der verschiedenen Schadsoftwaretypen stark variiert[110]. Als problematisch erweist sich in diesem Kontext auch die Tatsache, dass zwischen dem Zeitpunkt des Bekanntwerdens einer Schwachstelle bis zu ihrer Ausnutzung durchschnittlich sechs Tage verstreichen, was erhöhte Anforderungen an die Anbieter von Sicherheitssoftware einerseits und die IT-Abteilungen in Unternehmen andererseits stellt (Manthei, Schmidt 2005, 74)[111].

Ausgehend von dieser Einordnung ist dieses Kapitel wie folgt aufgebaut. In Abschnitt 4.1 werden die begrifflichen Grundlagen zum IT-Risiko gelegt. Darauf folgend werden in Abschnitt 4.2 die IT-Schutzziele näher erläutert, die vielfach herangezogen werden, um Auswirkungen dieser Art von Risiken zu beschreiben bzw. Anforderungen an IT-Systeme zu definieren. IT-RM, das im Vergleich zum traditionellen RM einer stärkeren Ressourcenfokussierung folgt, wird in Abschnitt 4.3 erläutert. Da der Themenbereich IT-RM sehr breit ist und eine hohe Varietät an IT-Systemen besteht, werden in

[109] Im Rahmen verschiedener Regularien wie z.B. Basel II ist ein expliziter Umgang mit IT-Risiken gefordert. Bezüglich Basel II kann somit IT-Sicherheitsmanagement dazu beitragen, die für operationelle Risiken zu hinterlegende Eigenkapitalmenge zu reduzieren (Hirschmann, Romeike 2004, 18).

[110] Siehe hierzu auch die aktuellen Studien durch die Hersteller von Antivirus Software z.B. (Gostev 2007).

[111] Nach Schätzungen der Radicati Group (http://www.radicati.com/) entstanden durch Angriffe auf Arbeitsplätze in 2006 ein Schaden von 54 Mrd. $ (Licari 2005, 45).

Abschnitt 4.4 ausgewählte Standards vorgestellt, die einen Beitrag zum systematischen Umgang mit dieser komplexen Aufgabe leisten. Das Kapitel schließt mit einer zusammenfassenden Betrachtung und einer Diskussion der bedeutendsten Aspekte (siehe 4.5).

4.1 IT-Risiko

Während im traditionellen RM Risiko als Erwartungswert aus Eintrittswahrscheinlichkeit und Schadensausmaß gesehen wird, wird im IT-RM vielfach die Auffassung vertreten, dass ein Risiko daraus entsteht, dass eine bestimmte Bedrohung eine oder mehrere Schwachstellen ausnutzt (Peltier 2001, 21; Alberts, Dorofee 2003, 13; Suh, Han 2003, 150; Yapp 2003, 174; Müßig 2006, 36; Windemann et al. 2006, 53). Diese Unterscheidung ist bedeutend, da Unternehmen einerseits vielfältigen Bedrohungen ausgesetzt sind, aber andererseits in unterschiedlichem Ausmaß durch diese Bedrohungen verwundbar sind.

Hinsichtlich der Kategorisierung von Bedrohungen besteht weitgehend Einigkeit. So wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der IT-Grundschutzkataloge (siehe 4.4.2) eine Einteilung der Bedrohungen in (1) höhere Gewalt, (2) organisatorische Mängel, (3) menschliche Fehlhandlungen, (4) technisches Versagen und (5) vorsätzliche Handlungen vorgenommen. Die Kategorien und die jeweils zugeordneten Einzelbedrohungen sind der Klassifikation nach Basel II ähnlich, wobei bei Personen eine Unterscheidung zwischen Vorsatz und Fehlhandlungen die Bedeutung der Intention ausdrückt (BSI 2006, 16, 304 ff). Die besondere Bedeutung der Intention hebt auch Dierstein hervor (Dierstein 2004, 343f). So bestehen einerseits absichtlich herbeigeführte Bedrohungen, die weiterhin in aktive und passive Angriffe unterteilt werden können. Erstere können z.B. in Form von Eingriffen in die Datenübertragung, Überlasterzeugung, Sabotage, Vortäuschung falscher Identitäten oder Einbringen von Schadsoftware auftreten. Passive Angriffe betreffen z.B. das Abhören von Daten oder die Analyse des Verkehrsflusses. Darüber hinaus können Bedrohungen auch unabsichtlich herbeigeführt werden und dabei auf menschliches Fehlverhalten, mangelhafte oder veralterte Systeme, Umwelteinflüsse oder auch Naturkatastrophen zurückgehen (Bitkom 2003, 13). Im Hinblick auf Angriffe auf IT-Systeme kann in direkte und indirekte Angriffe unterschieden werden, wobei erstere auf die Überwindung bzw. Lahmlegung vorhandener Sicherheitsfunktionalität abzielen, während durch indirekte Angriffe Sicherheitsmechanismen umgangen werden sollen (Kruth 2004, 200). Dabei liegen Ursachen wie Stromausfälle, Blitzschläge oder Angriffe externer Personen zum Teil nicht in der jeweiligen Einflusssphäre des Unternehmens, während fahrlässiges oder mutwilliges Verhalten der Mitarbeiter in der Einflusssphäre liegt (Baer, Zängerle 2000, 68).

Einen Überblick über die Zusammenhänge der verschiedenen Begriffe im Bereich IT-RM bietet auch die Norm ISO/IEC 15408 (siehe Abb. 18). Demnach stellen Ressourcen für Eigentümer einen Wert dar, weshalb Risiken, die diese werthaltigen Ressourcen betreffen, minimiert werden sollen. Zu diesem Zweck ergreifen die Eigentümer bestimmte Maßnahmen zur Erhöhung der IT-Sicherheit, wobei Risiken dadurch zustande kommen, dass Bedrohungen vorhanden sind und das Unternehmen bzw. die jeweilige Ressource für diese Bedrohung verletzbar ist. Bedrohungen können neben Systemen oder höherer Gewalt auch von Personen, wie z.B. böswilligen Nutzern oder Hackern, ausgehen, die die Ressourcen missbrauchen bzw. dem Unternehmen gezielt einen Schaden zufügen möchten. Von diesem Motiv ausgehende Bedrohungen nutzen dabei Schwachstellen oder bedrohen die Ressourcen selbst. Die zentrale Steuergröße zur Vermeidung von Risiken stellt damit die Ergreifung von Maßnahmen dar, wobei zu beachten ist, dass auch diese nicht frei von Schwachstellen sein können (CC 2006c, 35).

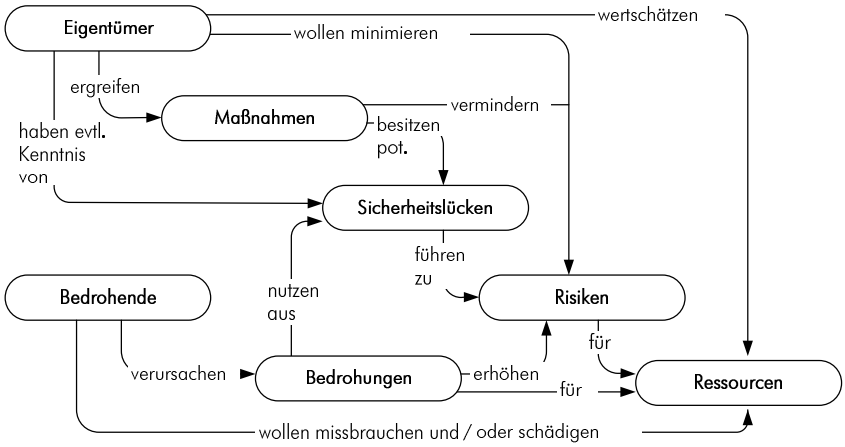


Abb. 18 Begriffsnetz zu Risiken ISO/IEC 15408[112]

Basierend auf dieser Abgrenzung wird nachfolgend eine Betrachtung verschiedener Definitionen zu IT-Risiko vorgenommen. Wolf sieht IT-Risiken als Teil der operationellen Risiken nach Basel II und definiert IT-Risiko als eine mit einem Verlust einhergehende Abweichung eines aktuellen von einem geplanten Ergebnisses, das mit einer bestimmten Eintrittswahrscheinlichkeit und einem unsicheren Schadensausmaß verbunden ist. Ursachen von IT-Risiken stellen dabei das Versagen der IT-Systemen selbst, der Prozesse, der Personen, die diese entwickeln, betreiben oder nutzen, oder externe Ereignisse dar (Wolf 2005, 51).

Junginger nimmt in Anlehnung an das Lebenszyklusmodell des Informationsmanagements eine Kategorisierung von IT-Risiken vor. Dabei schließt der Lebenszyklus Personal, Software, Hardware und Information als Ressourcen ein und besteht aus den Phasen Portfolio-, Projekt-, Produkt- und Infrastrukturmanagement sowie der Festlegung und Umsetzung der Strategie als übergeordnete Aufgabe. IT-Risiken werden demzufolge entsprechend der Phasen in Portfolio-, Projekt-, Betriebs-, Überwachungs- sowie Strategie- und Führungsrisiken unterteilt (Junginger 2005, 137ff).

[112] Eine ähnliche Abgrenzung ist auch bei (CC 2006c, 35) zu finden.

Eine weitere Kategorisierung erfolgt nach dem Prüfstandard IDW PS 330, der durch das Institut der Wirtschaftsprüfer herausgegeben wurde, im Rahmen der Jahresabschlussprüfung eingesetzt wird und speziell auf (rechnungslegungsbezogene) IT-Systeme fokussiert ist. In diesem Prüfstandard wird eine Unterteilung in IT-Infrastruktur-, IT-Anwendungs- und IT-Geschäftsprozessrisiken vorgenommen (IDW 2001, Tz 20ff). Erstere ergeben sich daraus, dass die für die Informationsverarbeitung notwendige IT-Infrastruktur nicht bzw. nicht in dem erforderlichen Maße zur Verfügung steht. IT-Anwendungsrisiken entstehen aus (a) fehlerhaften Funktionen in IT-Anwendungen, (b) fehlenden oder nicht aktuellen Verfahrensregelungen und -beschreibungen, (c) unzureichend ausgeprägten Eingabe-, Verarbeitungs- und Ausgabekontrollen von Daten in IT-Anwendungen sowie (d) nicht ausreichenden Maßnahmen zur Gewährleistung der Softwaresicherheit im Zusammenhang mit der Sicherheitsinfrastruktur. IT-Geschäftsprozessrisiken als dritte IT-Risikokategorie werden durch fehlende Sicherheits- und Ordnungsmäßigkeitsanalysen in Geschäftsprozessen verursacht (IDW 2001, Tz 20ff). Romeike differenziert IT-Risiken in organisatorische Risiken (z.B. mangelnder Schutz von Daten vor unautorisiertem Zugriff), projektbezogene Risiken (z.B. Termin- oder Kostenüberschreitungen), kosten- und leistungsbezogene Risiken (z.B. Kostenbelastung durch Risikoträger), infrastrukturelle Risiken (z.B. fehlende physische Sicherungsmaßnahmen) sowie anwendungs- und prozessbezogene Risiken (z.B. Schnittstellenprobleme) (Romeike 2000, 603f).

Eine alternative Kategorisierung sieht eine Unterteilung in Störungs-, Sicherheits- und Medienrisiken vor. Störungsrisiken betreffen dabei die Nichtverfügbarkeit der gesamten Infrastruktur, Netzverbindungen oder einzelner Systeme. Unter Sicherheitsrisiken werden Verletzungen der Vertraulichkeit und Unversehrtheit der Daten subsumiert, die beispielsweise durch das Ausspionieren, böswillige Veränderung oder Zerstörung verursacht werden kann (Lesch, Richter 2000, 1774f). Unter Medienrisiken werden die Verletzung von Urheber-, Patent- und Markenrechten, wettbewerbsrechtliche Verstöße, Domain-Streitigkeiten sowie Verletzung fremder Persönlichkeitsrechte subsumiert (Koch 2005, 111f).

Über die verschiedenen Kategorisierungen hinweg wird die Bandbreite der IT-Risiken durch die IT-Wertschöpfungstiefe[113] bestimmt, die den Grad, zu dem IT-Leistungen unternehmensintern erbracht werden, beschreibt (Seibold 2006, 26f). Dabei nimmt die Bandbreite der potentiellen Risiken mit zunehmender Wertschöpfungstiefe zu.

Im Folgenden wird der Auffassung von Wolf gefolgt und IT-Risiken als Teil der operationellen Risiken gesehen. Dabei können die Risiken den Kategorien Personen, Prozesse, Systeme und externe Ereignisse zugeordnet werden und sind auf die Ebene der operativen Geschäftsprozesse fokussiert.

[113] Die Wertschöpfungstiefe wirft auch Fragen der Versicherbarkeit auf. Koch unterscheidet bezogen auf den Betreiber der Systeme auf IT-Eigen- und IT-Fremdschadensrisiken (Koch 2005, 113ff).

4.2 IT-Schutzziele

Bei der Verarbeitung, Speicherung und Übermittlung von Informationen ist es erforderlich, dass Sicherheitsaspekte erfüllt werden. Dies bedeutet, dass von der IT mehrere Grundeigenschaften erwartet werden, die ihre Präzisierung in den so genannten IT-Schutzzielen[114] gefunden haben (Humpert 2004, 7). Dabei werden Vertraulichkeit, Integrität, Authentifikation und Verfügbarkeit als Basisziele bezeichnet und durch Dienste eines IT-Systems umgesetzt (Hansen, Neumann 2005, 285f). Während im Hinblick auf die Basisziele in der Literatur weitgehend Einigkeit vorhanden ist, bestehen im Hinblick auf die darauf basierenden höheren Ziele Abweichungen. So variieren diese entweder bezüglich ihrer Bezeichnung oder unterscheiden sich im Hinblick auf das Granularitätsniveau. Entsprechende Unterschiede werden bei der nachfolgenden Diskussion erläutert und konsolidiert. Als höhere Ziele werden Authentizität, Nicht-Abstreitbarkeit, Zugriffskontrolle, Zurechenbarkeit und Revisionsfähigkeit sowie Anonymisierung bzw. Pseudomisierung in diesem Abschnitt genannt, die ebenso wie die Basisziele durch entsprechende Dienste der IT-Systeme unterstützt werden (Rannenberg 2000, 490; Bitkom 2003, 15; Hansen, Neumann 2005, 285f; Eckert 2006, 6ff; Gordon, Loeb 2006, 121). Abb. 19 gibt einen Überblick über die verschiedenen Schutzzielen, die im Folgenden detailliert werden.

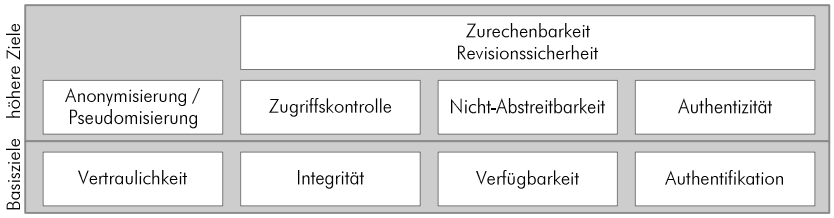


Abb. 19 Übersicht zu IT-Schutzzielen

Vertraulichkeit bezeichnet das Ziel, dass Informationen durch unautorisierte Personen nicht zugänglich und vor unbeabsichtigter Veröffentlichung geschützt sind. Bezogen auf ein IT-System liegt Vertraulichkeit dann vor, wenn keine unautorisierte Informationsgewinnung möglich ist (Peltier 2001, 5; Bitkom 2003, 14; Hansen, Neumann 2005, 286; Eckert 2006, 8f). Integrität stellt darauf ab, zu verhindern, dass zu schützende Daten manipuliert werden können. Dadurch soll die Ursprünglichkeit der Daten erhalten bleiben und auch nachweisbar sein (Peltier 2001, 4; Bitkom 2003, 14; Hansen, Neumann 2005, 286; Eckert 2006, 8; Gordon, Loeb 2006, 121). Durch das Basisziel Verfügbarkeit wird das Bestreben ausgedrückt, dass Systeme oder Dienste auch einem Nutzer zur Verfügung stehen und nicht aufgrund übermäßiger Beanspruchung o.ä. nicht nutzbar sind. Verfügbarkeit ist also dann gewährleistet, wenn ein System oder Dienst in einem definierten Zeitraum antwortet bzw. bestimmte Aktionen auslöst (Peltier 2001, 5; Bitkom 2003, 14; Hansen, Neumann 2005, 287; Eckert 2006, 10f). Weiterhin bezeichnet Authentifikation die Identifikation einer Person, die IT-Ressourcen nutzen möchte, und soll gewährleisten, dass

[114] Als alternative Bezeichnung wird zum Teil auch der Begriff Sicherheitsziel verwendet.

diese auch diejenige ist, die sie vorgibt zu sein. Im Falle von IT-Systemen spricht man von Benutzerauthentifikation (Hansen, Neumann 2005, 287).

Hinsichtlich der höheren Schutzziele besteht in der Literatur keine Einigkeit. Vielfach wird Zurechenbarkeit bzw. Verbindlichkeit als viertes oder aggregiertes Schutzziel genannt (Rannenberg 2000, 490; Eckert 2006, 11). In diesem Kontext wird allerdings wie auch in Abb. 19 dargestellt, eine feinere Unterscheidung vorgenommen und neben den Basiszielen auch Authentizität, Nicht-Abstreitbarkeit und Zugriffskontrolle als Voraussetzung für Zurechenbarkeit angesehen (Hansen, Neumann 2005, 286ff). Unter Authentizität eines Objektes[115] versteht man dessen Echtheit und Glaubwürdigkeit, die anhand seiner eindeutigen Identität und seiner charakteristischen Eigenschaften überprüfbar ist (Bitkom 2003, 15; Eckert 2006, 7). Nicht-Abstreitbarkeit ist ein höheres Ziel, das gewährleistet, dass bezüglich einer übermittelten Nachricht weder der Absender das Versenden noch der Empfänger den Erhalt negieren können (Hansen, Neumann 2005, 288). Zugriffskontrolle setzt die Authentifikation eines Benutzers voraus und fordert, dass dem jeweiligen Nutzer nur diejenigen Aktionen gewährt werden, zu denen er legitimiert ist (Hansen, Neumann 2005, 289). Zurechenbarkeit wird auch zum Teil als Verbindlichkeit bezeichnet und setzt Authentizität, Zugriffskontrolle und Nicht-Abstreitbarkeit voraus. Durch die mit dem Ziel korrespondierenden Dienste erfolgt eine Protokollierung der Inanspruchnahme der Ressourcen, was zur Folge hat, dass Aktionen einer auslösenden Instanz (Person oder System) zugerechnet werden können (Hansen, Neumann 2005, 289; Eckert 2006, 11f; Gordon, Loeb 2006, 121). Revisionsfähigkeit ist gleichlaufend mit der Zurechenbarkeit, betont jedoch deren rechtliche Durchsetzbarkeit. So soll gewährleistet werden, dass alle für den Rechtsverkehr (z.B. Haftung und Gerichtsfestigkeit) in Systemen und Netzen verwendeten Informationen und Vorgänge gegenüber Dritten nachweisbar sind (z.B. im Rahmen einer Wirtschaftsprüfung) (Bitkom 2003, 15). Anonymisierung bzw. Pseudomisierung haben zum Ziel, die Identität des jeweiligen Benutzers zu schützen. Anonymisierung bedeutet in diesem Kontext, dass personenbezogene Daten so verändert werden, dass Angaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugerechnet werden können. Pseudomisierung ist eine schwächere Variante, mittels derer personenbezogene Daten durch eine Zuordnungsvorschrift so verändert werden, dass die Angaben über persönliche und sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können (Eckert 2006, 12f). Die IT-Schutzziele definieren Anforderungen an IT-Systeme und sind somit auch für IT-RM von Bedeutung. Im Hinblick auf das Management von Wissensrisiken sind diese Anforderungen von Relevanz, wenn Geschäftsprozesse, die Wissen verarbeiten, IT-gestützt sind, da insbesondere in Bezug auf dokumentiertes Wissen Analogien bestehen.

[115] Objekte sind in diesem Zusammenhang z.B. Web-Server, Access Points oder Daten.

4.3 IT-Risikomanagement

Die Begriffe Sicherheit und Risiko sind interdependent. So stellt Risiko eine Funktion aus Eintrittswahrscheinlichkeit und Schadensausmaß eines unerwünschten Ereignisses dar, während Sicherheit als Freiheit von unvertretbarem Risiko bezeichnet werden kann (Mock 2003, 167f). Sicherheit kann somit als Ergebnis der Begrenzung der Risikolage bzw. des Ergreifens bestimmter Maßnahmen sein (Farny 1979, 12ff; Thiel 2004, 53). Aufgrund dieser Interdependenz werden auch die Begriffe IT-Risiko- und IT-Sicherheitsmanagement in der Literatur vielfach synonym verwendet, wobei in diesem Kontext erstgenannter Begriff zugrunde gelegt wird, da er umfassender ist und neben dem sicheren Betrieb der IT-Systeme auch Qualitätsaspekte und Wirtschaftlichkeitsbetrachtungen einschließt (Junginger, Krcmar 2001, 396; Book, Rudolph 2005, 55; Seibold 2006, 33ff). Insbesondere der Schutz von Informationen, der durch die IT-Schutzziele konkretisiert wird, ist bei der Entwicklung dieser Disziplin immer weiter in den Vordergrund gerückt (Dierstein 2004, 351; Windemann et al. 2006, 51).

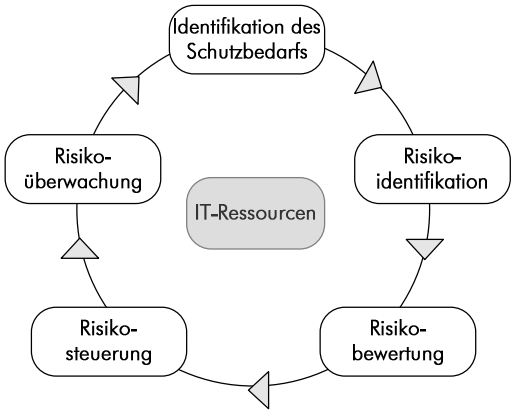


Abb. 20 Kernaufgaben des IT-RM

Der IT-RM-Prozess (siehe Abb. 20) ist an den traditionellen RM-Prozess (siehe Abschnitt 3.5) angelehnt und deckt sich im Wesentlichen mit den Kernaufgaben Risiken identifizieren, bewerten, steuern und überwachen (Krcmar 2005, 444ff). Diese Kernaufgaben schlagen sich auch im Standard ISO/IEC 13335 nieder, in dem neben dem WM-Prozess u.a. auch die organisatorische Verankerung des IT-RM erörtert werden (Bitkom 2006, 23). Dem IT-RM-Prozess wird durch die strategische Sicherheitspolitik des Unternehmens in der Form von Zielen, Richtlinien und Grundsätzen eine Richtung vorgegeben, wobei die Ausrichtungen variieren können (Sitzberger, Nowey 2006, 159). So kann vorwiegend der Schutz nach außen angestrebt werden, während die Sicherheitsmaßnahmen innerhalb des Unternehmens niedrig gehalten werden. Dabei legt dieser Ansatz eine umfassende Vertrauensdomäne im Unternehmen zugrunde. Diese Vertrauensdomäne wird im Falle einer prozessbasierten Sicherheitsstrategie auf die Instanzen eines einzelnen Prozesses (z.B. Abteilung, Team) verkleinert. Dies bedeutet, dass im Rahmen dieser Grundausrichtung auch zwischen Prozessen unternehmensintern Sicherheitsmaßnahmen ergriffen werden und somit die Zugänglichkeit zu Informationen begrenzt wird. Die vollkommene Auflösung der unternehmensinternen Vertrauensdomäne resultiert aus dem Verfolgen der Strategie Sicherheit nach innen und außen. Dabei wird jede Information unabhängig von Prozessen und Instanzen als schützenswert definiert. Zu beachten ist dabei, dass mit zunehmender Begrenzung der Vertrauensdomäne auch das Misstrauen zwischen Abteilungen und Mitarbeitern indirekt gefördert wird (Schmidt 2006, 87f). Auf der operativen Ebene erfolgt unter Zugrundelegung der Grundausrich-

tung die Ableitung eines Sicherheitskonzeptes, von dem wiederum einzelne Maßnahmen abgeleitet werden (Sitzberger, Nowey 2006, 159). Nachfolgend werden auf Basis der strategischen Ausrichtung die Besonderheiten der einzelnen Prozessphasen kurz erläutert.

Identifikation des Schutzbedarfs: Eine Erweiterung im Vergleich zum traditionellen RM besteht in einigen Ansätzen zum IT-RM darin, dass ein expliziter Einbezug bzw. eine Voranalyse der betroffenen Ressourcen im Hinblick auf den Schutzbedarf erfolgt. IT-Ressourcen schließen nach einem weiten Verständnis Hardware, Software, Daten, Personal und Gebäude ein (Suh, Han 2003, 152; Humpert 2004, 8). Dabei besteht eine zentrale Aufgabe darin, zu analysieren, welche Informationen kritisch und schutzbedürftig und somit in die Betrachtungen des IT-RM einzubeziehen sind (Queensland 2001, 8; Alberts, Dorofee 2003, 35ff; Suh, Han 2003; Yapp 2003, 174). Die Ermittlung dieses Schutzbedarfes orientiert sich dabei am Wert der IT-Ressourcen, der sich seinerseits aus der Bedeutung für den Eigentümer ergibt. Zur Beurteilung der Bedeutung kann die Ausprägung der IT-Schutzziele herangezogen und daraus ein Maßstab festgelegt werden (Pohlmann 2006, 27).

Risikoidentifikation: Es besteht eine Vielzahl an Analysen im Kontext des Managements von IT-Risiken, die komplementär sind und somit zur Entwicklung eines Gesamtüberblicks beitragen. Beispiele sind Zielanalysen zur Festlegung der Sicherheitsziele, Strukturanalysen zur Erfassung der IT-Landschaft, Ist-Analysen zur Darstellung der ergriffenen Sicherheitsmaßnahmen und Risikoanalysen zur Bewertung von Eintrittswahrscheinlichkeiten und Schadensausmaßen (Humpert 2004, 9ff; Eckert 2006, 151ff). Eine umfassende und weit verbreitete Analyse stellt in diesem Kontext auch die Business-Impact Analyse dar, bei der der Gesamtausfall der IT und die Auswirkungen auf die Geschäftsfelder betrachtet werden. Dabei werden Beeinträchtigungen der Aufgabenerfüllung, potentielle Imageverluste, finanzielle Auswirkungen sowie Verstöße gegen Gesetze oder Vorschriften berücksichtigt (Gerick 2004, 13).

Risikobewertung: Die klassische Risikobewertung im Sinne von Abschnitt 3.5.3, die die Bildung von Erwartungswerten beinhaltet, ist im Falle des IT-RM nicht geeignet. Dies liegt v.a. daran, dass Eintritts- bzw. Ausfallwahrscheinlichkeiten schwer zu ermitteln sind. Selbst wenn Wahrscheinlichkeiten für ein Teilsystem ermittelt werden können, sind vielfach Aussagen in Bezug auf das Gesamtssystem nur schwer zu treffen, was vorwiegend auf die Komplexität der IT-Systeme zurückzuführen ist. Es besteht eine Vielzahl an Schadensereignissen, die aufgrund ihrer Anzahl kaum zu beschreiben sind (Baer, Zängerle 2000, 68f). Aufgrund der Komplexität und des Variantenreichtums der IT-Systeme und der daraus resultierenden Anzahl potentieller Schadensereignisse werden im Rahmen des IT-RM vielfach Grundschutzansätze verfolgt. Diese verzichten auf eine detaillierte Analyse von Risiken und die Bildung von Erwartungswerten und fordern auf der Basis eines Soll-Ist Vergleiches das Ergreifen von Sicherheitsmaßnahmen. In den letzten Jahren hat sich ein Trend zur Prävention ergeben, da es kostengünstiger ist, negative Ereignisse zu vermeiden anstelle Wiederherstellungen vorzunehmen,

Vertrauensverluste oftmals nicht wiederhergestellt werden können und zudem nahezu keine geeigneten Versicherungslösungen bestehen (Young 2002, 3). Dabei kommt neben dem Ergreifen von präventiven Maßnahmen dem umfassenden Einsatz von organisatorischen Richtlinien (Policies) eine immer stärkere Bedeutung zu (Manthei, Schmidt 2005, 76).

Risikosteuerung: Das IT-RM geht weit über technische Maßnahmen hinaus, was auch insbesondere durch zahlreiche Schnittstellen zu anderen Fachgebieten wie physische Sicherheit, Recht, Disaster und Business Recovery, IT-Assetmanagement, Compliance (z.B. Audit-Richtlinien, Basel II) und Corporate Governance (z.B. SOX, KonTraG) deutlich wird (Lubich 2006, 7). Es bestehen verschiedene Ansätze zur Kategorisierung der Steuerungsmaßnahmen. So kann eine Einteilung in die vier Kategorien Wiederherstellung, Entdeckung, Zusicherung und Vermeidung erfolgen (Young 2002, 5). Maßnahmen der erstgenannten Kategorie zielen dabei auf die Wiederherstellung von Systemen nach Störvorfällen ab, während Maßnahmen zur Entdeckung z.B. das unautorisierte Eindringen in Netzwerke aufdecken sollen. Maßnahmen im Bereich der Zusicherung umfassen beispielsweise die Protokollierung, während Firewalls oder Verschlüsselung Maßnahmen zur Vermeidung darstellen (Young 2002, 5). Als zusätzliche Kategorie können Maßnahmen zur Abschreckung angeführt werden, die beispielsweise Sicherheitsrichtlinien für Mitarbeiter oder Zugangskontrollen einschließen (Straub, Welke 1998, 444f).

Eine weitere verbreitete Unterteilung ist die Klassifikation in organisatorische, technische und rechtliche Maßnahmen. Organisatorische Maßnahmen betreffen beispielsweise die Herausgabe von Richtlinien sowie die Sicherstellung deren Einhaltung oder die Schaffung von Sicherheitsbewusstsein, während technische Maßnahmen Fragen des Zugriffs, der Systemsicherheit oder Verschlüsselung zum Gegenstand haben. Bei einer weiter gefassten Sichtweise und dem Einbezug von Gebäuden als Ressource schließt diese Kategorie auch bauliche Maßnahmen ein. Rechtliche Maßnahmen würdigen arbeits-, zivil- und strafrechtliche Aspekte und setzen gesetzliche Verpflichtungen, wie z.B. den Schutz personenbezogener Daten oder Kundendaten, entsprechend um (Hansen, Neumann 2005, 285; Schmidt 2006, 97)[116].

Risikoüberwachung: Eine Grundproblematik im IT-RM ist darin zu sehen, dass einerseits sensitive Informationen in Netzwerken vorliegen und andererseits Software und Systeme nicht frei von Fehlern sind. Bedeutend ist dabei, dass die Aufwendungen für die Schutzmaßnahmen mit der Effizienz der Maßnahmen, den Gefährdungen und dem Wert der zu schützenden Ressourcen stehen (Matousek et al. 2004, 33). Eine absolute Sicherheit gegen Angriffe ist dabei nahezu nicht zu gewährleisten, weshalb das primäre Ziel der IT-Sicherheit darin besteht, die Hürden für Angriffe möglichst hoch zu halten (Manthei, Schmidt 2005, 76). Zudem besteht ein Zielkonflikt zwischen der Nutzbarkeit der IT-

[116] Für eine detaillierte Übersicht zu Steuerungsmaßnahmen im Kontext der IT-Sicherheit wird auf einschlägige Werke wie z.B. (BSI 2006; Eckert 2006) verwiesen.

Systeme einerseits und deren Sicherheit andererseits, der zur Folge hat, dass je System eine Abwägung der Sicherheitsmaßnahmen im Hinblick auf den finanziellen Aufwand und den für die Umsetzung erforderlichen Zeitbedarf erfolgen muss (Hansen, Neumann 2005, 285).

Bezüglich der Kosten- und Nutzenbetrachtung ist das IT-RM durch mehrere Probleme gekennzeichnet. Bedingt dadurch, dass Sicherheitsvorfälle mit einer bestimmten Wahrscheinlichkeit eintreten, sind die auf die ergriffenen Sicherheitsmaßnahmen zurückzuführenden Ersparnisse im Sinne von ausbleibenden Schäden nur schwer zu belegen und verursachungsgerecht zuzurechnen (Gadatsch, Uebelacker 2006, 45; Lubich 2006, 8; Schadt 2006, 17). Zur Beurteilung der Effizienz der eingesetzten Sicherheitsmaßnahmen kann der Return on Security Investment (ROSI) herangezogen werden. Vereinfacht kann diese Kennzahl als Summe aus Ertrag und Kostenersparnis, die zu den getätigten Investitionen in Relation gesetzt wird, beschrieben werden. Die Kostenersparnisse entsprechen der Vermeidung von Verlusten, während sich der Ertrag aus Ersparnissen ergibt, die ohne Sicherheitsinvestitionen nicht zu realisieren sind. Ersparnisse sind z.B. auf die Reduzierung bzw. den Nichteintritt von Kosten wahrscheinlicher Schäden zurückzuführen. Die Investitionen entsprechen den Kosten, die mit den Sicherheitsmaßnahmen verbunden sind und schließen neben Anschaffungskosten auch Kosten für Schulung, Betrieb, Wartung und Ersatz ein (Matousek et al. 2004, 37; Lubich 2006, 11; Pohlmann 2006, 27) [117].

Das Problem dieser Kennzahl ist allerdings darin zu sehen, dass sehr präzise Rechnungen auf der Basis grober Schätzungen gemacht werden. Daher ist die Varianz der Ergebnisse hoch und muss stark branchen- bzw. firmenspezifisch angepasst werden (Lubich 2006, 12). Augrund der zum Teil schlechten Datenbasis z.B. in Bezug auf die Zahl vereitelter Sicherheitsvorfälle oder die Effektivität der Sicherheitsmaßnahmen hat der ROSI vielfach nur eine geringe Aussagekraft (Matousek et al. 2004, 37).

Aufgrund der schweren Rechtfertigbarkeit von Investitionen in IT-Sicherheit, werden Investitionen in Unternehmen vielfach erst dann getätigt, wenn unverhältnismäßig hohe Schäden eingetreten sind (Schadt 2006, 17). Soll jedoch einem Risiko, das für das Unternehmen inakzeptabel ist, entgegengewirkt werden, so werden unabhängig von ROI-Betrachtungen und der Amortisationszeiten Sicherheitsmaßnahmen ergriffen (Gadatsch, Uebelacker 2006, 46; Schadt 2006, 20).

Im konkreten Anwendungsfall variiert die Ausgestaltung des IT-RM stark, wobei einige Teilaspekte wie Identitäts-, Zugangsmanagement, Entwicklung und Integration, Bedrohungsmanagement oder Management der Sicherheitsinformation Minimalmaßnahmen darstellen (Lubich 2006, 6f).

Aufgrund der Vielzahl an Analysen und Maßnahmen sowie der Heterogenität der IT-Systeme werden in folgendem Abschnitt Standards zum systematischen Management der IT-Sicherheit vorgestellt, die dieser Heterogenität Rechnung tragen.

[117] Eine Berechnung des ROSI in Bezug auf die Amortisationszeit bei Anschaffung einer Software für Festplattenverschlüsselung ist bei Pohlmann zu finden. Für Details siehe (Pohlmann 2006, 31ff).

4.4 Ausgewählte Standards zum IT-Risikomanagement

Wie in den Abschnitten (4.1-4.3) dargestellt, ist die Etablierung eines leistungsfähigen IT-RM eine komplexe Aufgabe, da eine Vielzahl an Betrachtungsobjekten zu integrieren sind. So werden neben der gesamten Hardware in der Form von Arbeitsplatzrechnern, Servern, Netzwerken sowie mobilen Endgeräten auch Anwendungen einbezogen. Darüber hinaus stellen Personen und die bauliche Infrastruktur eines Unternehmens ebenso Betrachtungsgegenstände dar. Aufgrund dieser Breite und der hohen Varietät ist eine systematische Unterstützung des IT-RM erforderlich.

Zahlreiche Standards leisten einen Beitrag zur Systematisierung und Lösung dieser komplexen Aufgabe, indem sie die Implementierung eines IT-RM auf den verschiedenen Strategieebenen unterstützen. Als Standard wird in diesem Kontext eine Richtlinie, Vorgabe oder Konvention bezeichnet, die durch Autorität, Gewohnheit oder Konsens als Vorschrift für Beurteilungen oder das Handeln breit anerkannt wird (Teubner, Terwey 2005, 96) Standards werden in der Regel durch eine anerkannte Institution, wie z.B. das Deutsche Institut für Normung (DIN) oder die International Organization for Standardization (ISO), bestätigt und basieren auf den konsolidierten Ergebnissen der Wissenschaft und Technologie (De Vries 2006, 4). Diese Aussagen treffen allerdings nur auf so genannte „de jure“ Standards zu. Daneben bestehen auch „de facto“ Standards, die durch einzelne bzw. mehrere Unternehmen erarbeitet und nicht von einer bestimmten unabhängigen Institution verabschiedet werden (Rada 2000, 6). Standards haben zum Vorteil, dass sie auf dem aktuellen Stand von Technik und Wissenschaft, praxiserprobt und oftmals weit verbreitet sind und somit gewissermaßen Best Practices darstellen. Durch ihre Anwendung kann neben der Erfüllung gesetzlicher Anforderungen, wie z.B. KonTraG oder SOX, auch die Vergleichbarkeit und Nachvollziehbarkeit verbessert werden. Zudem bieten „de jure“ Standards die Möglichkeit einer Zertifizierung, die wiederum ein entscheidendes Differenzierungsmerkmal gegenüber Wettbewerbern darstellen kann (Bitkom 2005, 6).

Erste Ansätze zur Entwicklung von Standards zum IT-RM haben nachrichtendienstlichen Ursprung und gehen auf das Orange Book zurück, das Anfang der 80’er Jahre vom National Institute of Standards and Technology (NIST) entwickelt wurde (Junginger 2005, 142). Zum aktuellen Zeitpunkt hat sich allerdings noch kein Universalstandard, der die ganze Realität abbildet, entwickelt. Es bestehen vielmehr mehrere Standards, die unterschiedliche Schwerpunkte aufweisen, zum Teil partiell und in Kombination mit anderen Standards in Unternehmen eingesetzt werden. Oftmals erfolgt eine Ergänzung um unternehmensspezifische Anforderungen (Schmidt 2006, 100). Neben der Unterstützung der Risikoanalyse durch die Definition eines Vorgehens und eines Analysewerkzeuges soll die Steuerung der Risiken durch eine Sammlung an Best Practice Sicherheitsmaßnahmen unterstützt werden.

In diesem Abschnitt werden ausgewählte Standards betrachtet, wobei als Auswahlkriterien deren Ausrichtung und Bekanntheitsgrad herangezogen werden. Bezüglich Ausrichtung werden Standards fokussiert, die über technische Fragestellungen hinausgehen, da IT-RM vorwiegend auch ein organisato-

risches bzw. ein Managementproblem darstellt (Hirschmann, Romeike 2004, 13) und dies v.a. auch auf das Management von Wissensrisiken als zentralen Betrachtungsgegenstand dieser Arbeit zutrifft. Dieser Ausrichtung folgen die komplementären Standards ISO/IEC 17799 und ISO/IEC 27001 (siehe 4.4.1) sowie die IT-Grundschutzkataloge (siehe 4.4.2). Zudem werden die Common Criteria (siehe 4.4.3) kurz dargestellt, die auf die Evaluierung von IT-Produkten bezogen sind. CobiT, als weit verbreiteter „de facto" Standard, zielt auf die Verbesserung des Kontrollsystems ab und verfügt über ein Rahmenwerk, das eine ganzheitliche Sicht der IT einnimmt (siehe 4.4.4). Zudem besteht mit SOMAP (siehe 4.4.5) auch im Open-Source Bereich ein Standard, der aufgrund der Kostenvorteile für viele Unternehmen ebenfalls von Relevanz ist und daher gesondert betrachtet wird.

4.4.1 ISO/IEC 17799 / ISO/IEC 27001

Die Standards BS 7799 und ISO/IEC 17799 verfolgen einen Best Practice Ansatz und stellen einen Leitfaden zum Aufbau und Führen eines Informationssicherheits-Managementsystems (ISMS) dar. Unter Leitung des britischen „Departments of Trade and Industry" wurden 1989 in Zusammenarbeit mit Unternehmen eine Verhaltensrichtlinie („Users Code of Practice") entwickelt und in den Folgejahren weiterentwickelt. 1995 wurde der darauf basierende Standard BS 7799-1 durch das British Standard Institute (BSI) verabschiedet. In 2001 erfolgte die Überführung in einen international verbindlichen Standard, ISO/IEC 17799[118]. Neben BS 7799-1 besteht noch ein zweiter Teil des British Standards (BS 7799-2), durch den beschrieben wird, wie ISO/IEC 17799 anzuwenden ist.

Überwachungsbereiche
IT-Sicherheitsleitlinie
Organisation der Informationssicherheit
Management von Ressourcen
personelle Sicherheit
physische und umgebungsbezogene Sicherheit
Betriebs- und Kommunikationsmanagement
Zugriffskontrolle
Beschaffung, Entwicklung und Wartung
Management von Sicherheitsvorfällen
Geschäftskontinuitätsplanung
Einhaltung der Verpflichtungen

Tab. 5 Überwachungsbereiche nach ISO/IEC 17799

Dabei werden die Anforderungen für Erstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten ISMS unter Berücksichtigung der Risiken innerhalb der gesamten Organisation spezifiziert. In 2005 wurde BS 7799-2 in ISO/IEC 27001 überführt[119] (Junginger 2005, 146f; Hofmann 2006, 206ff).

Durch ISO/IEC 17799 werden Sicherheitsanforderungen definiert, die dann von Relevanz sind, wenn Schutzbedarf für Informationen besteht. Die Maßnahmen sind allgemein abgefasst, weshalb eine Anpassung an die Spezifika des Unternehmens erforderlich ist. Dabei werden 11 Überwachungsbereiche (siehe Tab. 5) für Richtlinien und Maßnahmen definiert, die das ISMS in Bezug auf die Initiierung,

[118] Die vollständige aktuelle Bezeichnung lautet (ISO/IEC 17799:2005 - Information technology - Code of practice for information security management)

[119] Aufgrund der Bestrebungen, alle Standards, die ISMS betreffen, als ISO/IEC 27000er-Reihe zusammenzuführen, soll ISO/IEC 17799 ab 2007 in ISO/IEC 27002 umbenannt werden.

Umsetzung und Verbesserung unterstützen. Diese werden wiederum in 39 Hauptkategorien, so genannte Kontrollziele untergliedert, zu deren Erreichung 133 Sicherheitsmaßnahmen unterlegt sind (Bitkom 2006, 25f). Eine Zertifizierung nach ISO/IEC 17799 ist grundsätzlich nicht möglich. Soll ein ISMS zertifiziert werden, kann dies nur nach ISO/IEC 27001 erfolgen. Dabei kann das Erfüllen der Anforderungen bzgl. der Umsetzung des ISMS von internen oder externen Auditoren überprüft werden (Bitkom 2006, 25)[120].

4.4.2 IT-Grundschutzkataloge

Die IT-Grundschutzkataloge[121] wurden aufgrund der zunehmenden Gefährdung in einer ersten Version 1995 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht. Es stellt in mehreren Katalogen Methodiken und praktische Umsetzungshilfen zur Etablierung eines kontinuierlichen und effektiven IT-RM-Prozesses bereit.

Das Ziel der Grundschutzkataloge besteht darin, durch infrastrukturelle, technische, organisatorische und personelle Standardmaßnahmen ein Sicherheitsniveau zu erreichen, das ein Mindestmaß an Sicherheit, also einen so genannten Grundschutz, bietet, um somit eine ausbaufähige Basis zu schaffen. Aufgrund der ausgeprägten Heterogenität der in der Praxis eingesetzten IT-Systeme folgen die IT-Grundschutzkataloge einem Baukastenprinzip, das unterschiedlichsten Systemen und Anwendungen Rechnung tragen soll (BSI 2006, 14). Die Erstellung eines IT-Sicherheitskonzeptes wird dadurch erleichtert, dass keine Risikoanalyse im klassischen Sinne erforderlich ist, sondern ein Soll-Ist-Vergleich zwischen empfohlenen und ergriffenen Maßnahmen durchgeführt wird (BSI 2006, 14). Hinsichtlich der Maßnahmen erfolgt eine Unterscheidung in solche, die zur Erfüllung der Minimalanforderungen erforderlich sind und zusätzlichen Maßnahmen, die sich in der Praxis bewährt haben (BSI 2006, 14).

Die IT-Grunschutzkataloge sind in Bausteine, Gefährdungs- und Maßnahmenkataloge gegliedert (siehe Tab. 6), die untereinander vernetzt sind.

Bausteine	Gefährdungskataloge	Maßnahmenkataloge
• (B1) übergeordnete Aspekte der IT-Sicherheit • (B2) Sicherheit der Infrastruktur • (B3) Sicherheit der IT-Systeme • (B4) Sicherheit im Netz • (B5) Sicherheit in Anwendungen	• (G1) höhere Gewalt • (G2) organisatorische Mängel • (G3) menschliche Fehlhandlungen • (G4) technisches Versagen • (G5) vorsätzliche Handlungen	• (M1) Infrastruktur • (M2) Organisation • (M3) Personal • (M4) Hard- und Software • (M5) Kommunikation • (M6) Notfallvorsorge

Tab. 6 zentrale Elemente der IT-Grundschutzkataloge

Bausteine detaillieren die betrachteten Komponenten, Vorgehensweisen und IT-Systeme, wobei die entsprechenden Gefahren und Standardmaßnahmen referenziert werden. Durch die Gefährdungskataloge werden Gefährdungen entsprechend ihrer Kategorisierung mit den einzelnen Bausteinen in Be-

[120] Weitere Details siehe auch (Völker 2005).
[121] In den Versionen 1996-2005 wurden die IT-Grundschutzkataloge "IT-Grundschutzhandbuch" genannt.

ziehung gesetzt. Maßnahmen aus unterschiedlichen Bereichen werden innerhalb der Maßnahmenkataloge betrachtet und mit den beiden anderen Elementen vernetzt (BSI 2006, 14). Das BSI ermöglicht eine mehrstufige Zertifizierung. Die beiden Selbsterklärungen IT-Grundschutz-Einstiegsstufe und IT-Grundschutz-Ausbaustufe können ohne Beteiligung Dritter von den Zeichnungsbefugten der jeweiligen Institution vorgenommen werden. Für die Erteilung eines IT-Grundschutz-Zertifikates bedarf es eines Audit-Reports eines lizenzierten IT-Grundschutz-Auditors (Bitkom 2005, 13).

4.4.3 Common Criteria

Die Common Criteria[122] sind ein internationaler Standard (ISO/IEC 15408) zur Bewertung und Zertifizierung der Sicherheit von IT-Produkten. Als IT-Produkte werden in diesem Standard Hard-, Soft- und Firmware bezeichnet (CC 2006c, 9). Dazu werden im Standard Kriterien zur Evaluierung der Datensicherheit und des Datenschutzes definiert, die vorwiegend auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (siehe Abschnitt 4.2) fokussiert sind. Der Standard findet dabei sowohl für die Entwicklung von IT-Produkten mit Sicherheitsfunktionalität als auch bei deren Beschaffung Anwendung (CC 2006c, 9). Die Common Criteria, die aktuell in der Version 3.1 vorliegen, zielen auf eine Vereinheitlichung und Weiterentwicklung der europäischen ITSEC[123], der kanadischen CTCPEC[124] und der amerikanischen TCSEC[125] ab. Der Standard soll somit eine international einheitliche Grundlage zur Prüfung und Zertifizierung bieten. Durch die positive Prüfung wird der Nachweis erbracht, dass alle Sicherheitsanforderungen an die IT-Produkte vollständig erfüllt sind und nicht durch Schwachstellen im System umgangen werden können. Zentrale Oberpunkte für Prüfkriterien sind der Funktionsumfang und die Vertrauenswürdigkeit. Die Common Criteria bieten die Möglichkeit, Sicherheitsanforderungen in vorevaluierten Schutzprofilen zusammenzufassen. Diese stellen unabhängig von der Implementierung eine Beschreibung der Sicherheitsanforderungen an bestimmte Typen von IT-Produkten dar und können somit auf verschiedene Instanzen (Produkte) des entsprechenden Typs angewandt werden (CC 2006c, 16, 40). Diese Schutzprofile umfassen ein Sicherheitskonzept und eine Auflistung der Bedrohungen, denen IT-Produkte ausgesetzt sind. Daneben bestehen so genannte Sicherheitsziele (Security Targets), die in Abhängigkeit der Implementierung eines konkreten IT-Produkts Sicherheitsanforderungen spezifizieren. Sie dienen somit der Überprüfung der Erfüllung der allgemeinen Sicherheitsanforderungen aus den Schutzprofilen und werden durch die Hersteller umgesetzt bzw. dienen der Zertifizierungsstelle als Evaluierungsbasis (CC 2006c, 17, 30).
Die Common Criteria bestehen aus drei Teilen.

[122] Die vollständige Bezeichnung lautet: Common Criteria for Information Technology Security Evaluation.
[123] Information Technology Security Evaluation Criteria
[124] Canadian Trusted Computer Product Evaluation Criteria
[125] Trusted Computer System Evaluation Criteria werden auch als Orange Book bezeichnet.

- Teil 1 dient zur Einführung und zur Darstellung der Definitionen des allgemeinen Modells und des Geltungsbereiches. Zudem werden Schutzprofile und Sicherheitsziele beschrieben.
- Teil 2 umfasst die Definition funktionaler Sicherheitsanforderungen. Diese stellen eine Empfehlung zur Beschreibung der Funktionalität eines IT-Produkts dar. Dabei werden die Anforderungen verschiedener Funktionsklassen, wie z.B. Sicherheitsprotokollierung, Kommunikation, Schutz der Nutzerdaten, Unterstützung der Verschlüsselung oder Authentifizierung, zugeordnet. Dabei sind die Anforderungen zielgruppenspezifisch für Entwickler und Auditoren differenziert (CC 2006a, 18ff).
- Teil 3 definiert Anforderungen an die Vertrauenswürdigkeit, die die Korrektheit der Implementierung des betrachteten Systems bzw. die Prüftiefe beschreiben. Dabei bestehen verschiedene Klassen an Kriterien, wie z.B. Entwicklung, Dokumentation, Unterstützung des Lebenszyklus oder Evaluierung der Sicherheitsziele. Es erfolgt dabei eine Unterteilung in sieben Stufen, die von „funktionell getestet“ als niedrigste bis hin zu „formal verifizierter Entwurf und getestet“ als höchste Vertrauenswürdigkeitsstufe reichen (CC 2006b, 30ff).

Neben der Verbesserung der unternehmensinternen IT-Sicherheit, kann der Beitrag der Common Criteria zur Risikoreduktion insbesondere auch in der interorganisationalen Zusammenarbeit gesehen werden, da durch die Zertifizierung Kunden, Lieferanten und Partnern ein hoher Sicherheitsstandard gewährleistet werden kann (Junginger 2005, 148).

4.4.4 CobiT

CobiT (Control Objectives for Information and Related Technology) ist ein international anerkannter Standard zur IT-Governance und soll ein Bindeglied zwischen Risiko, IT sowie Prüfungs- und Kontrollanforderungen schaffen (Junginger 2005, 149). Der „de facto“ Standard berücksichtigt seinerseits wiederum über 40 international anerkannte Standards (Rentschler 2005, 26). CobiT wurde 1993 durch die Information Systems Audit and Control Association (ISACA), einem internationalen Verband der die Interessen von IT-Fachleuten in den Bereichen Prüfung, Überwachung und Sicherheit vertritt, entwickelt und 1996 als Werkzeug angeboten. Seit 2000 ist das IT-Governance Institute für die Weiterentwicklung von CobiT, das mittlerweile in der vierten Version vorliegt, zuständig. CobiT dient sowohl zur Steuerung der IT aus Unternehmenssicht als auch als Beurteilung der Reife, wobei eine formale Zertifizierung nicht möglich ist (Rentschler 2005, 26). CobiT basiert auf der Annahme, dass IT am besten gesteuert werden kann, wenn die in den Geschäftsobjekten benötigten Informationen den Ausgangspunkt darstellen. Dabei erfolgt eine Fokussierung auf die Wechselbeziehungen zwischen Unternehmenszielen und IT. So werden die Ziele einer Unternehmung durch die IT erst ermöglicht und auf der anderen Seite die Unternehmensziele mit Hilfe der IT umgesetzt. Zentral sind in diesem Zusammenhang die IT-Ressourcen, die die Geschäftsprozesse mit Informationen versorgen. Co-

biT folgt der Prozessorientierung, nimmt eine ganzheitliche Sicht auf die IT ein und strukturiert die IT in 34 Prozesse, die ihrerseits den Domänen Planung und Organisation, Beschaffung und Implementierung, Betrieb und Unterstützung sowie Überwachung zugewiesen sind. Je Prozess sind eine Prozessbeschreibung, das Ziel des Prozesses, die Aktivitäten, wesentliche Messgrößen, die Anforderungen und Handlungsempfehlungen definiert (IT-Governance-Institute 2005, 30ff).

Zentral sind dabei die Anforderungen (control objectives), mittels derer eine ausreichende Informationsversorgung der Geschäftsprozesse gewährleistet werden soll. Zentrale Anforderungen an Informationen stellen die Wirksamkeit, Wirtschaftlichkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance und Verlässlichkeit dar. Aus der Perspektive des Sicherheitsmanagements ist dabei insbesondere die Einhaltung der in Abschnitt 4.2 dargestellten Schutzziele von Bedeutung. Zudem ist die Anforderung Compliance, die die Einhaltung von Gesetzen, Richtlinien, Regularien oder vertraglichen Vereinbarungen einfordert, bei der Durchführung der Geschäftsprozesse bedeutend (IT-Governance-Institute 2005, 14). CobiT adressiert IT-Sicherheitsmanagement direkt und indirekt. So besteht explizit ein Prozess zum RM, der sich mit den in Abschnitt 3.5 erläuterten Kernaufgaben des RM deckt. Eine Nichtberücksichtigung bestimmter Maßnahmen geht nach dem Verständnis von CobiT mit IT-Risiken einher und stellt somit deren indirekte Adressierung dar (IT-Governance-Institute 2005, 67ff; Book, Rudolph 2005, 58).

Durch Audit-Richtlinien wird der Stand der Implementierung überprüfbar und im Rahmen des zugehörigen CobiT-Reifegradmodells mit sechs Reifestufen, z.B. nicht-existent, definierter Prozess oder optimiert, differenziert bewertbar und somit der Fortschritt in der Implementierung messbar (Bitkom 2006, 36).

4.4.5 SOMAP

Neben den vorgestellten Standards bestehen auch im Open Source Bereich Bestrebungen zum IT-RM. Dies wird beispielsweise durch das Security Officers Management and Analysis Project (SOMAP) vorangetrieben[126]. Das Projekt hat zum Ziel, die Risikoanalyse und Steuerung von IT-Risiken insbesondere durch einen Katalog an Best Practice Maßnahmen sowie ein Werkzeug zur Risikoanalyse zu unterstützen (Wiesmann 2006, 65). SOMAP umfasst mehrere Bestandteile, die auch von kommerziellen Standards abgedeckt werden. Mittels eines Handbuchs soll das grundlegende Verständnis zum RM geschaffen werden. Zentrale Begriffe werden definiert und gegeneinander abgegrenzt. Ebenso werden die einzelnen Schritte, die im Rahmen der Risikoanalyse erforderlich sind, in einem zweiten Handbuch beschrieben. Zudem besteht eine Sammlung an Best Practices zu Sicherheitsmaßnahmen in Form eines Repository, während darüber hinaus mittels Vorlagen für Reports die Risikoanalyse unterstützt wird. Das Projekt befindet sich aktuell noch in Entwicklung.

[126] Siehe auch http://www.somap.org/.

In Abgrenzung zu kommerziellen Anbietern ist für SOMAP wie auch für andere Open Source Projekte kennzeichnend, dass den verteilt gesammelten Inhalten eine Struktur fehlt und dadurch die Operationalisierung in Unternehmen erschwert wird. Andererseits hat die verteilte Sammlung der Inhalte zum Vorteil, dass die Weiterentwicklung des Ansatzes gefördert wird und nicht wie bei vielen kommerziellen Standards zum Teil langwierig ist (Wiesmann 2006, 66). Als besonders positiv kann die Open Source Entwicklung des Tools zur Risikoanalyse beurteilt werden, da in diesem Zusammenhang Synergien zu vermuten sind.

Neben den angeführten Standards im Bereich ISMS besteht eine Vielzahl an spezialisierten Standards, die die Erstellung eines IT-Sicherheitskonzeptes bzw. die Umsetzung von IT-Sicherheitsmaßnahmen unterstützen. Für eine detaillierte Übersicht wird auf den Kompass zu IT-Sicherheitsstandards verwiesen, der durch Bitkom erstellt wurde[127].

4.5 Zusammenfassung und Diskussion

Im IT-RM besteht die Auffassung, dass sich Risiken aus dem Zusammentreffen einer Bedrohung und einer Schwachstelle ergeben. Hinsichtlich der unterschiedlichen Kategorien für Bedrohungen besteht weitgehend Einigkeit. So werden in den IT-Grundschutzkatalogen ähnlich wie im Falle operationeller Risiken nach Basel II höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen als Bedrohungskategorien herangezogen, wobei eine feinere Unterscheidung im Hinblick auf die Intention erfolgt und somit in Vorsatz und Fehlverhalten unterschieden wird. Ein besonderes Augenmerk ist bei Bedrohungen auch auf die Mitarbeiter zu richten, da die kostenintensivsten IT-Risiken unternehmensintern ausgelöst werden und somit eine zu starke Außenfokussierung zu einer verzerrten Betrachtung führen würde. Analog zu den Bedrohungen können IT-Risiken auch an die Risikoauffassung nach Basel II angelehnt werden und als eine Untergruppe operationeller Risiken verstanden werden, die sich über die verschiedenen Kategorien verteilt (Wolf 2005, 51). Somit werden IT-Risiken vorwiegend im Kontext operative Geschäftsprozesse gesehen.

Im Gegensatz zum traditionellen RM ist das IT-RM dadurch gekennzeichnet, dass vielfach eine ressourcenfokussierte Betrachtung verfolgt wird und IT-Ressourcen den zentralen Gegenstand darstellen. Dieser Fokussierung wird im Prozess des IT-RM vielfach durch eine explizite Berücksichtigung der Analyse der Schutzbedürftigkeit von IT-Ressourcen als eigene Phase Rechnung getragen. Hinsichtlich Bewertung erschweren die hohe Komplexität, Varietät und Interdependenzen im Kontext von IT-Systemen die Zuweisung konkreter Eintrittswahrscheinlichkeiten und Schadensausmaße. Aus diesem Grund werden die Bewertungsprobleme zum Teil durch ein präventives Vorgehen umgangen.

[127] Siehe hierzu auch (Bitkom 2006; Voßbein 2006).

Zudem schlägt sich diese Ressourcenfokussierung auch darin nieder, dass im IT-RM für die betroffenen Ressourcen Schutzziele definiert werden, die es zu erfüllen gilt. Weite Verbreitung haben in diesem Zusammenhang die Basisziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentifikation gefunden, die gewissermaßen Kernsicherheitsanforderungen an IT-Systeme darstellen. Zudem werden höhere Ziele definiert, die beispielsweise bei Geschäftstransaktionen von Bedeutung sind.

Die hohe Varietät der IT-Systemlandschaften und die Vielzahl potentieller Bedrohungen erfordert einen systematischen Umgang mit IT-Risiken, der durch eine Vielzahl an Standards unterstützt wird. Neben entsprechenden ISO-Standards, wie z.B. ISO/IEC 15408, ISO/IEC 17799 oder ISO/IEC 27001, bieten auch die IT-Grundschutzkataloge, CobiT oder SOMAP eine entsprechende Unterstützung. Bisweilen besteht allerdings kein Universalstandard, der das gesamte IT-RM abdeckt, was v.a. durch die hohe Varietät der IT-Systeme bzw. deren Komponenten und den daraus resultierenden erforderlichen Detaillierungsgrad bei Maßnahmen im Bereich Infrastruktur oder physische Sicherheit zu erklären ist. Aus diesem Grund werden in Unternehmen Kombinationen aus verschiedenen Standards, die jeweils eine unterschiedliche Ausrichtung aufweisen, eingesetzt.

5 Wissensrisiko und Wissensrisikomanagement

Der wissensbasierte Ansatz trägt der Zunahme der Wissensintensität von Produkten und Dienstleistungen Rechnung und stellt Wissen als die zentrale Ressource, die Wettbewerbsvorteile begründet, in den Vordergrund (Grant 1996b; Spender 1996). Eine Vielzahl an Ansätzen zielt darauf ab, die Effizienz des Einsatzes wissensbezogener Ressourcen zu erhöhen (z.B. Sveiby, Lloyd 1987; Wiig 1988; Barney 1991; Grant 1991; Nonaka 1991; Blackler 1995; Probst et al. 1998). Diese Ansätze haben u.a. zum Ziel, Wissen transparent zu machen, zu explizieren, zu kodifizieren und auch im Unternehmen oder über die Unternehmensgrenzen hinaus zu verteilen (siehe Kapitel 2). In den Ansätzen des WM wird nur selten thematisiert, wie Wissen gesichert werden kann, damit auch wissensbasierte Wettbewerbsvorteile nachhaltig gesichert werden können (Desouza, Vanapalli 2005, 76). Einige Autoren[128] heben in diesem Zusammenhang auch hervor, dass WM eine dunkle Seite aufweisen kann und die Transparenz des Wissens bzw. Einflussmöglichkeiten missbraucht werden können. So kann dokumentiertes Wissen verzerrt dargestellt werden, um im Kontext der Unternehmenspolitik bestimmte Interessen durchzusetzen. Weiterhin können Barrieren aufgebaut werden, um zu verhindern, dass Wissen, das diesen Interessen entgegensteht, angewandt wird. Zudem kann die durch die Aktivitäten des WM verursachte Transparenz missbraucht und zum Schaden des Unternehmens eingesetzt werden (Alter 2006, 2). Da Wissen selbst mit Unsicherheiten bzw. Nichtwissen verbunden ist, ist dessen Anwendung selbst schon mit Risiken behaftet (Strulik 2001, 38, 51). Einige Autoren heben auch konkret das Risiko des Scheiterns von WM-Projekten hervor. Lam und Chua bezeichnen dieses Scheitern als WM-Risiko und unterteilen diese Oberkategorie in technologische, kulturelle, inhaltliche Risiken sowie Risiken im Zusammenhang mit dem Projektmanagement. Gründe für das Scheitern sind beispielsweise eine zu hohe Komplexität der Technologie, eine geringe Aktualität der Inhalte oder ein unzureichender Einbezug der Mitarbeiter (Lam, Chua 2005, 427ff).

Obwohl RM seit langem als integraler Bestandteil der Unternehmensführung angesehen wird und die Risikoorientierung in den letzten zehn Jahren insbesondere auch durch die Regulation deutlich zugenommen hat (z.B. KonTraG, Basel II, SOX), weisen diese Ansätze ebenso wie die Literatur zum WM in der Regel keinen expliziten Einbezug von Risiken auf, die die Ressource Wissen betreffen. Vielmehr erfolgt eine primäre Betrachtung von Markt- und Kreditrisiken. Risiken, die die Ressource Wissen betreffen, sind daher in der Regel nicht Gegenstand der Risikokategorisierungen, die den entscheidenden Ausgangspunkt für deren Identifikation und die nachgelagerten Kernaufgaben des RM darstellen (siehe Kapitel 3). Allerdings werden, wenn auch nur vereinzelt, Aspekte, die Risiken in Bezug auf die Ressource Wissen betreffen, in der Literatur zum RM erörtert. Dies wird bei der nachfolgenden Herleitung des Konzeptes Wissensrisiko berücksichtigt. Zudem werden im Kontext des IT-

[128] Siehe hierzu (Alter 2006; Jennex 2006).

RM (siehe Kapitel 4) Risiken in Bezug auf Informationen bzw. dokumentiertes Wissen sowie Schutzziele (siehe 4.2) thematisiert und Maßnahmen zu deren Steuerung entwickelt. Aus diesem Grund ist auch dieser Forschungsbereich für das Management von Wissensrisiken relevant. Da der Ressource Wissen vielfach eine hohe Bedeutung für die Erbringung der Wertschöpfung und die Generierung der Wettbewerbsvorteile von Unternehmen beigemessen wird[129], ist eine Nichtbeachtung von Risiken als unzureichend anzusehen. Dies wird auch zum Teil in der Literatur zum WM eingefordert und so betont Jennex, dass eine integrierte Betrachtung erforderlich ist, da einerseits der Wert von Wissen im Rahmen der Forschung zum intellektuellen Kapital und der Bilanzierungsrichtlinien zunehmend wahrgenommen wird und zum anderen die Regulation in Bezug auf Risiken stetig voranschreitet (Jennex 2006, 3). Im Hinblick auf das intellektuelle Kapital empfiehlt Nemetz, eine Erweiterung der Berichterstattung vorzunehmen und auch Risiken explizit einzubeziehen. So können beispielsweise Risiken, die Human-, Struktur- und Beziehungskapital (siehe auch Abschnitt 2.3.1) betreffen, abgebildet und mit den traditionellen Berichten zum Wert bzw. den Modellen zur Wertbestimmung des intellektuellen Kapitals in Beziehung gesetzt werden, wobei der Eintritt eines Risikos die korrespondierenden Werte des intellektuellen Kapitals senkt (Nemetz 2006, 18f).

Aus genannten Gründen ist eine Integration dieser beiden Managementansätze zum Ansatz des Wissensrisikomanagements Gegenstand dieses Kapitels. Dazu werden Teilaspekte dieser beiden Ansätze auf Basis der Literatur integriert und in das Konzept Wissensrisiko überführt (siehe 5.1). Im Anschluss daran erfolgt eine Systematisierung des Konzeptes Wissensrisiko, das Ursachen und Wirkungen von Wissensrisiken in Beziehung zueinander setzt (siehe 5.2). Darauf basierend werden zu den vier Konzepten Wissensverlust (5.3), Wissensdiffusion (5.4), Wissenstransfer (5.5) und Wissensqualität (5.6) ausgehend von einer allgemeinen Betrachtung die aus der Literatur identifizierten Einzelrisiken erörtert und zudem exemplarisch Interaktionen zwischen diesen Risiken aufgezeigt. Neben konzeptinternen Interaktionen werden auch ausgewählte konzeptübergreifende Interaktionen betrachtet (5.7) und im Anschluss daran die zentralen Erkenntnisse diskutiert (5.8).

5.1 Das Konzept Wissensrisiko

Mit der integrierten Betrachtung der Konzepte Risiko und Wissen haben sich zum aktuellen Stand der Forschung nur wenige Autoren systematisch auseinandergesetzt. Zumeist werden in der Literatur einzelne Teilaspekte aufgegriffen. Ziel dieses Abschnittes ist es, die in der Literatur diskutierten Betrachtungen dieser beiden Konzepte zu verdichten und zum Konzept Wissensrisiko zu systematisieren.

Die erste explizite Auseinandersetzung mit Wissensrisiken im deutschsprachigen Raum erfolgte durch Probst und Knaese (1998, 27). Sie sehen das Risiko im Verlust an Know-how Kapital des Unterneh-

[129] Siehe hierzu (Grant 1996b, 375; von Krogh, Roos 1996, 32; Stewart 1998; Marsh, Ranft 1999, 43; Robertson, Hammersley 2000, 241; Zahn et al. 2000, 384).

mens, der durch den unerwünschten oder unfreiwilligen Abfluss, die Substitution, die Vernichtung, die Fehlallokation oder Nichtnutzung von kritischem Wissen verursacht werden kann (Probst, Knaese 1998, 27; ähnl. Zbinden, Meyer 2001). Dabei schließt diese Sichtweise sachlich-technische, personelle, organisatorische und marktbezogene Know-how-Risiken ein, wobei Knaese schwerpunktmäßig die mit der Personalfluktuation verbundenen Risiken betrachtet (Knaese 2004, 34ff, 129ff). Der personalwirtschaftliche Fokus dieser Definition schlägt sich dabei besonders auch in der Wahl der Risikoelemente Fehlallokation und Nichtnutzung nieder. Die Fehlallokation betrifft in diesem Kontext Risiken in Bezug auf Qualifikationsdefizite, Fehlinvestitionen in Weiterbildungsmaßnahmen etc. Derartigen Risiken kann durch eine gezielte Allokation von Wissensträgern begegnet werden. Auch die Nichtnutzung von Wissen stellt ein primär personalwirtschaftliches Problem dar, das auf Barrieren zurückzuführen ist und dem vorwiegend durch Ansätze der Motivation und Führung begegnet werden kann. Die Substitution von Wissen stellt ein im strategischen Management (vgl. Porter (1985) vielfach diskutiertes Risiko dar. Dabei scheint es schwer möglich, Risiken in Bezug auf die Substitution zu beeinflussen, da die Determinanten vielfach außerhalb des Einflussbereiches des Unternehmens liegen. Die Vernichtung von Wissen bezeichnet einen permanenten nicht wieder herstellbaren Verlust an Wissen, während der Abfluss von Wissen dessen Werthaltigkeit und somit die Wettbewerbsvorteile des Unternehmens negativ beeinflussen kann (Knaese 2004, 32ff). Diesen beiden Elementen wird auch im Kontext der vorliegenden Arbeit Bedeutung beigemessen. Da diese Definition eine vergleichsweise umfassende Betrachtung von Wissensrisiken vornimmt und gewissermaßen als erste vollständige Definition in der Literatur anzusehen ist, wird sie für die nachfolgende Erläuterungen herangezogen, um Unterschiede aufzuzeigen.

Auch Kobi verfolgt einen personalwirtschaftlichen Fokus und definiert Engpass-, Austritts-, Anpassungs- und Motivationsrisiken als die vier zentralen Personalrisikokategorien (Kobi 1999, 13ff). Das Austrittsrisiko stellt dabei auf den potentiellen Verlust von Mitarbeitern ab, während Engpässe auf Abhängigkeiten von einzelnen Mitarbeitern bzw. von Schwierigkeiten bzgl. der Personalbeschaffung gekennzeichnet sind. Anpassungsrisiken beziehen sich auf die fehlerhafte Qualifikation von Mitarbeitern und laufen somit mit Fehlallokationen im Sinne von Knaese gleich. Motivationsrisiken betreffen die Leistungsbereitschaft der Mitarbeiter, wobei die potentielle Nichtnutzung von Wissen nach der Abgrenzung von Knaese einen Teilaspekt dieser Risikokategorie darstellen kann (Kobi 1999, 13ff). Ebenso kann aus einer personalwirtschaftlichen Perspektive ein Risiko in der mangelnden Qualifikation der Mitarbeiter gesehen werden. So stehen beispielsweise die zur Durchführung der Aufgaben bzw. Projekte erforderlichen Kompetenzen nicht zur Verfügung oder reichen nicht aus (Keßler, Winkelhofer 2002, 162; Harrant, Hemmrich 2004, 18).

Amelingmeyer spricht nicht explizit von Wissensrisiken, setzt sich jedoch mit der Sicherung der Wissensbasis auseinander und hebt dabei die Bewahrung des Wissens vor Verlust, dessen Sicherung ge-

gen unerwünschte Nutzung sowie die Entfernung irrelevanten Wissens hervor (Amelingmeyer 2002, 146ff). Erstgenannter Punkt entspricht dabei dem Element Vernichtung nach Knaese. Auch die unerwünschte Nutzung läuft gleich mit dem ungewollten Abfluss. Die Entfernung irrelevanten Wissens stellt im Wesentlichen auf Wissen ab, das nicht mehr aktuell ist und somit einen geringeren Wert in Bezug auf die Bewirtschaftung darstellt.

Des Weiteren sehen Lindstaedt et al. (2004, 2) Wissensrisiken als Risiken, die sich auf einen Mangel von Wissen und Fähigkeiten, welche für die Durchführung einer geschäftsrelevanten Aktion notwendig sind, zurückführen lassen. Während Knaese sowohl strategische als auch operative Risiken[130] betrachtet, stellt der Wissensrisikobegriff von Lindstaedt et al. primär auf die operative Ebene ab. Diese Ausrichtung wird auch dieser Arbeit zugrunde gelegt, da einerseits eine Anwendung von Wissen im Tagesgeschäft erfolgt und andererseits Risiken auf der Ebene operativer Geschäftsprozesse bedingt durch weniger Einflussfaktoren und geringerer Komplexität vergleichsweise leichter zu steuern sind.

Mohamed et al. betrachten die Aspekte des Verlustes und des ungewollten Abflusses von sensitivem Wissen integriert[131] und stellen dabei insbesondere auf die wettbewerbsrelevanten Auswirkungen ab. Dabei legen die Autoren eine weite Sichtweise auf Risiken zugrunde und betonen, dass der Verlust bzw. Abfluss von Wissen einerseits negative Konsequenzen nach sich zieht, aber sich für das Unternehmen auch Chancen ergeben, vom Abfluss bzw. von Verlusten anderer Unternehmen zu profitieren (Mohamed et al. 2006, 3). Die Autoren betrachten primär personelle Wissensträger und unterscheiden zudem zwischen einem bewussten bzw. beabsichtigten und einem unbewussten bzw. unbeabsichtigten Verlust bzw. Abfluss von Wissen. Somit können Verluste an Wissen beispielsweise durch Fluktuation allgemein auftreten, während ein Abfluss von Wissen im Rahmen unternehmensübergreifender Projekte oder durch die Fluktuation zu Konkurrenten verursacht wird (Mohamed et al. 2006, 6f).

Liman betrachtet den Verlust von Know-how[132] als zentralen Untersuchungsgegenstand und sieht diesen als gerichtete Übermittlung bzw. Transferierung, die mit oder ohne Zustimmung der Geschäftsleitung erfolgen kann. Dabei wird der Aspekt Abfluss von Wissen im Sinne von Knaese unter den Begriff Verlust bewusst durch Liman subsumiert, um die wertmäßige Bedeutung hervorzuheben (Liman 1999, 41). Im Hinblick auf die Kenntnis der Geschäftsleitung kann zwischen einem regulären und einem irregulären Verlust an Know-how unterschieden werden. Ersterer liegt dann vor, wenn die Geschäftsleitung den Abfluss von Wissen bzw. Fähigkeiten explizit wahrnimmt bzw. bedingt dadurch, dass keine Gegenmaßnahmen ergriffen werden, diesem zustimmt. Ein irregulärer Verlust liegt hingegen dann vor, wenn dieser ohne Wahrnehmung bzw. ohne Zustimmung der Geschäftsleitung erfolgt. Beispiele für einen regulären Verlust sind das Ersetzen von veraltetem Wissen durch neues

[130] Siehe hierzu auch Abschnitt 3.3.

[131] Die Autoren bezeichnen das Konzept als „knowledge leakage“ (Mohamed et al. 2006, 3).

[132] Auch Liman (1999) wählt den Begriff Know-how aus Gründen der Wertabgrenzung. Wie zuvor bereits erwähnt, liegt dieser Arbeit die Prämisse zugrunde, dass sich die Aussagen auf Wissen mit einer gewissen Werthaltigkeit beziehen.

oder Kündigungen von Mitarbeitern durch die Geschäftsleitung, während Wirtschaftsspionage ein Beispiel für eine Ursache für einen irregulären Verlust ist (Liman 1999, 41ff).

Die Relevanz der Diffusion von sensitiven Inhalten wird bereits 1985 in einer Studie von Mansfield thematisiert. Im Ergebnis der Studie zeigt sich, dass Entwicklungsentscheidungen von Wettbewerbern in einem Zeitraum von 12-15 Monaten wahrgenommen werden. Bei einem Fünftel der betrachteten Unternehmen erfolgt dies in einem Zeitraum unter sechs Monaten. Informationen zu neuen Produkten bzw. Prozessen sind bei Wettbewerbern innerhalb von 12 Monaten vorhanden und bei einem Drittel der betrachteten Unternehmen in einem Zeitraum unter sechs Monaten (Mansfield 1985, 221). Die Variabilität in den betrachteten Branchen ist hoch. Eine Korrelation mit der Imitationsgeschwindigkeit verneint Mansfield, da die Basisinformationen vielfach nicht ausreichend sind, um ein imitiertes Produkt bzw. eine Dienstleistung auf den Markt zu bringen (Mansfield 1985, 221). Stellt man die Studie in den zeitlichen Kontext, so ist anzunehmen, dass neue Technologien diese Zeiten nochmals reduziert haben.

Als weiterer Vertreter setzt sich Loomans (2004, 44) mit Informationsrisiken auseinander und versteht darunter die Gelegenheit oder Wahrscheinlichkeit, dass ein Unternehmen durch den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen einen Schaden erleidet. Diese Definition lässt sich auch auf dokumentiertes Wissen übertragen. Insbesondere der potentielle Verlust an Vertraulichkeit[133] ist von Relevanz für das Thema Wissensrisiko, da sich Wettbewerbsvorteile von Unternehmen auf exklusive wissensbezogene Ressourcen gründen und diese negativ beeinträchtigt werden können.

Alberts und Dorofee (2003, 95) definieren als mögliche Risiken in Bezug auf IT-Ressourcen Bekanntgabe, Verlust, Modifikation und Unterbrechung. Während die ersten beiden Elemente mit den Risikokategorien von Knaese korrespondieren, stellen die Modifikation und die Unterbrechung bzw. Nichtverfügbarkeit eine Ergänzung dar, die sich negativ auf die Qualität des vorhandenen Wissens auswirken kann. Da IT-Systeme bei der Durchführung von Geschäftsprozessen eine immer wichtigere Rolle einnehmen, kann die Anforderung an die Verfügbarkeit weit reichen und sogar eine Abhängigkeit vorliegen, wenn die Geschäftsprozesse durch die IT determiniert werden (Hirschmann, Romeike 2004, 13; Belsis et al. 2005, 189; Wolf 2005, 1).

Coleman und Casselman betrachten ebenso den Begriff Wissensrisiko und nehmen eine Unterteilung in wissensgefährdende und wissensbasierte Risiken vor. Erstgenannte fokussieren auf den potentiellen Verlust von Wissen, während wissensbasierte Risiken sich auf fehlendes bzw. mangelhaftes Wissen gründen und von den Autoren als Wissenslücken bezeichnet werden. Aus einer entscheidungsorientierten Perspektive kann somit die mangelnde Qualität des Wissens selbst sowie dessen fehlende Zugänglichkeit die Entscheidung negativ beeinträchtigen (Coleman, Casselman 2004, 5, 12ff). Im Hin-

[133] Siehe hierzu auch die IT-Schutzziele in Abschnitt 4.2.

blick auf die Durchführung wissensintensiver Aktivitäten ist es bedeutend, dass das dokumentierte Wissen eine hohe Qualität aufweist, um zu verhindern, dass beispielsweise fehlerhaftes Wissen durch Mitarbeiter internalisiert wird, Fehlentscheidungen getroffen oder das Wissen in die Produkte des Unternehmens inkorporiert wird.

Da Unternehmen aus Zeit- und Aufwandsgründen oftmals nicht in der Lage sind erforderliches Wissen selbst zu generieren, stellt der unternehmensübergreifende Wissenstransfer eine bedeutende Wissensquelle dar (Badaracco 1991, 123; Grant, Baden-Fuller 1995, 17ff; Husman 2001, 3; Escribá-Esteve, Urra-Urbieta 2002, 331). In diesem Kontext ist der Erfolg des Wissenstransfers relevant, also eine möglichst hohe Replikation des Wissens des Senders beim Empfänger. Dabei wird der Erfolg des Wissenstransfers durch verschiedene Barrieren negativ beeinflusst, was zur Folge hat, dass er unzureichend ist und erforderliches Wissen nicht in ausreichendem Maß zur Verfügung steht. Aggregiert betrachtet können die Barrieren spezifische Charakteristika des Senders, Empfängers, transferierten Wissens und des Kontexts betreffen und den Wissenstransfererfolg hemmen. Im Hinblick auf den Sender kann z.B. eine mangelnde Motivation angeführt werden, während eine empfängerseitige Barriere die mangelnde Fähigkeit zur Aufnahme und Integration des transferierten Wissens darstellt. Hemmende Faktoren in Bezug auf das transferierte Wissen stellen eine hohe Komplexität oder Spezifität des Wissens dar, während übermäßiges Schutzverhalten eine Barriere in Bezug auf den Kontext darstellt (Schüppel 1996, 107ff; Szulanski 1996, 30ff; Larsson et al. 1998, 291; Szulanski et al. 2003, 144; Lucas 2005, 87f; Riege 2005, 23ff)[134]. Da der externe Wissenstransfer aufgrund der kurzen Halbwertszeit und Innovationszyklen von Wissen vielfach eine wichtige Quelle für den Wissenserwerb darstellt, kann ein unzureichender Wissenstransfer Risiken in sich bergen. Im anglo-amerikanischen Raum werden seit langem Risiken im Kontext von interorganisationalen Arrangements wie strategischen Allianzen oder Joint Ventures thematisiert (Hamel et al. 1989; Hamel 1991; Bleeke, Ernst 1993; Lei 1993; Das, Teng 1999; Davies 2000). In der zumeist dem strategischen Management zuordenbaren Literatur stellen dabei v.a. die Auswirkungen des ungewollten bzw. unbeabsichtigten Abflusses von wettbewerbsrelevantem Wissen auf die Wettbewerbsposition bzw. die Wettbewerbsvorteile der Unternehmen den Betrachtungsgegenstand dar.

Nachfolgend werden die erörterten Aspekte, die auch in Tab. 7 zusammengefasst sind, nochmals in Zusammenhang der verschiedenen Vertreter diskutiert und im Anschluss daran in das Konzept Wissensrisiko überführt. Ausgehend von der Wissensrisikodefinition lassen sich aus der Literatur die vier Wissensrisikoursachen Verlust, unerwünschte Diffusion, unzureichender Wissenstransfer und eingeschränkte Wissensqualität als vergleichsweise verbreitet identifizieren, wobei die Elemente Substitution, Nichtnutzung und Fehlallokation nur in geringem Maße aufgegriffen werden.

[134] Für eine detaillierte Betrachtung der verschiedenen Einflussfaktoren auf den Wissenstransfererfolg wird auf Abschnitt 5.5.1 verwiesen.

Element der Wissens-risikodefinition	Vertreter
Verlust	• Vernichtung / Verlust von Wissen (allg.) (Liman 1999, 41f; Amelingmeyer 2002, 146ff; Knaese 2004, 32ff) • Verlust von personengebundenem Wissen (Kobi 1999, 13f; Mohamed et al. 2006, 3) • Verlust von Informationen / dokumentiertem Wissen (Alberts, Dorofee 2003, 95)
unerwünschte Diffusion	• unerwünschter Abfluss (Knaese 2004, 32ff) • Verlust von Wissen im Sinne eines Abflusses (Liman 1999, 41f) • unerwünschte Nutzung (Amelingmeyer 2002, 146ff) • Abfluss von Wissen durch Personen (Kobi 1999, 13f; Mohamed et al. 2006, 3) • Abfluss sensitiver Informationen über technologische Entwicklungen (Mansfield 1985, 221) • Offenlegung vertraulicher Informationen / dokumentierten Wissens (Alberts, Dorofee 2003, 95; Loomans 2004, 44) • ungewollter Abfluss von Wissen in interorganisationalen Arrangements (Hamel et al. 1989; Hamel 1991; Bleeke, Ernst 1993; Lei 1993; Das, Teng 1999; Davies 2000) • Dilemma zwischen Wissenstransfer und Wissensdiffusion (Hamel et al. 1989, 136; Sanchez 1995, 3; Baughn et al. 1997, 104; Appleyard, Kalsow 1999, 288; Kale et al. 2000, 217; Mitchell et al. 2002, 3; Mohr, Sengupta 2002, 282; Norrman, Lindroth 2004, 610; Oxley, Sampson 2004, 723)
unzureichender Transfer	• Barrieren, die den Wissenstransfererfolg hemmen o Charakteristika des Senders o Charakteristika des Empfängers o Charakteristika des transferierten Wissens o Charakteristika des Kontexts (Schüppel 1996, 107ff; Szulanski 1996, 30ff; Larsson et al. 1998, 291; Szulanski et al. 2003, 144; Lucas 2005, 87f; Riege 2005, 23ff)
eingeschränkte Qualität	• mangelnde Qualifikation personeller Wissensträger (Keßler, Winkelhofer 2002, 162; Harrant, Hemmrich 2004, 18; Knaese 2004, 32ff) • Entscheidungen auf der Basis von Wissen mit mangelhafter Qualität (Coleman, Casselman 2004, 5, 12ff) • mangelnde Integrität von Informationen / dokumentiertem Wissen (Alberts, Dorofee 2003, 95; Loomans 2004, 44) • mangelnde Zugänglichkeit zu Informationen (Alberts, Dorofee 2003, 95; Loomans 2004, 44) • Engpassrisiko aufgrund von Abhängigkeiten von Mitarbeitern (Kobi 1999, 13) • Abhängigkeit von IT-Systemen (Hirschmann, Romeike 2004, 13; Belsis et al. 2005, 189; Wolf 2005, 1)

Tab. 7 Elemente der Wissensrisikodefinition

Verlust: Der Verlust von Wissen als Element des Konzeptes Wissensrisiko stellt eine Ursache von Wissensrisiken dar und kann sowohl personelle als auch nicht-personelle Wissensträger[135] betreffen (Amelingmeyer 2002, 146ff; Knaese 2004, 32ff). Dabei können diese Verluste sowohl beabsichtigt als auch unbeabsichtigt erfolgen. Somit sind Verluste nicht zwingend als negativ zu betrachten, sondern können durchaus erwünscht sein. Dies trifft beispielsweise auf das Vergessen bzw. gezielte Verlernen[136] von veraltetem Wissen zu, da sich dessen Relevanz bzw. Wert für das Unternehmen reduziert hat. Demzufolge werden Verluste also dann als negativ angesehen, wenn sie unbeabsichtigt erfolgen

[135] Siehe hierzu Abschnitt 2.2.3.
[136] Siehe hierzu z.B. (Lyles et al. 2002; Akgün et al. 2007).

und es sich zudem um werthaltiges Wissen handelt[137] (Liman 1999, 41f; Amelingmeyer 2002, 148f; Desouza, Awazu 2005, 49ff). Neben der allgemeinen Betrachtung des Verlustes fokussieren einige Autoren speziell Verluste von personengebundenem Wissen, die z.B. durch die Fluktuation von Mitarbeitern zu anderen Unternehmen bzw. durch deren Ausscheiden aus dem Berufsleben verursacht werden (Kobi 1999, 13f; Mohamed et al. 2006, 3). Im Bereich des IT-RM wird primär der Verlust von Informationen bzw. dokumentiertem Wissen als Risikoursache behandelt (Alberts, Dorofee 2003, 95).

Unerwünschte Diffusion: Unter dem Wissensrisikoelement unerwünschte Diffusion lassen sich verschiedenste Aspekte zusammenführen. Wie auch im Falle des Wissensverlustes kann die Diffusion personelle und nicht-personelle Wissensträger betreffen (Amelingmeyer 2002, 146ff; Knaese 2004, 32ff). In Bezug auf personengebundenes Wissen kann eine unerwünschte Diffusion beispielsweise durch die Abwanderung der Mitarbeiter zu Konkurrenten erfolgen (Kobi 1999, 13f; Mohamed et al. 2006, 3), während im Hinblick auf dokumentiertes Wissen dessen Offenlegung oder der unzureichende Schutz vor dem Zugriff nicht autorisierter Personen eine Spezifizierung dieser Ursachenkategorie darstellen kann (Alberts, Dorofee 2003, 95; Loomans 2004, 44). Im internationalen Kontext ergeben sich Wissensrisiken dieser Ursachenkategorie aus der Schwierigkeit, dass Unternehmen abwägen müssen, inwiefern sie ihren Partnern Wissen zugänglich machen. So ist es einerseits im Hinblick auf die erwünschten Wissenstransferprozesse erforderlich, dass Partner Zugang zu Wissen erhalten und ein reger Austausch zwischen den Mitarbeitern besteht. Auf der anderen Seite bergen umfassender Zugang bzw. intensive Zusammenarbeit Risiken der ungewollten Diffusion von Wissen in sich. Somit besteht zwischen dem Erfolg des Wissenstransfers und der Wissensdiffusion ein Trade-off, der vielfach als Dilemma charakterisiert wird (Hamel et al. 1989, 136; Sanchez 1995, 3; Baughn et al. 1997, 104; Appleyard, Kalsow 1999, 288; Kale et al. 2000, 217; Mitchell et al. 2002, 3; Mohr, Sengupta 2002, 282; Norrman, Lindroth 2004, 610; Oxley, Sampson 2004, 723).

Unzureichender Transfer: Externer Wissenstransfer ist für Unternehmen eine bedeutende Option des Wissenserwerbs, da eine unternehmensinterne Entwicklung des Wissens vielfach an Kosten und Aufwand scheitert. Dabei wird allerdings dessen Erfolg durch eine Reihe von Barrieren wie beispielsweise Abwehr-, Vermeidungshaltungen des Empfängers, geringe Verlässlichkeit des Senders, hohe Spezifität des Wissens, mangelnder Kontext oder kulturelle Barrieren negativ beeinträchtigt (Schüppel 1996, 107ff; Szulanski 1996, 30ff; Larsson et al. 1998, 291; Szulanski et al. 2003, 144; Lucas 2005, 87f; Riege 2005, 23ff). Da bedingt durch mangelnden Erfolg des Wissenstransfers das benötigte Wissen nicht in ausreichender Form zur Verfügung steht, stellt ein unzureichender Wissenstransfer eine weitere Ursache für Wissensrisiken dar.

[137] Amelingmeyer diskutiert spezifische Maßnahmen, die ergriffen werden können, um nicht relevantes bzw. veraltetes Wissen aus der Wissensbasis zu entfernen (Amelingmeyer 2002, 149ff).

Eingeschränkte Qualität: Die eingeschränkte Qualität wissensbezogener Ressourcen als weitere Ursache von Wissensrisiken kann einerseits auf die mangelnde Qualifikation der Mitarbeiter zurückgeführt werden, die sich auf die Durchführung der Aufgaben negativ auswirkt (Keßler, Winkelhofer 2002, 162; Harrant, Hemmrich 2004, 18). Andererseits kann sie durch die mangelnde Integrität von in IT-Systemen verwaltetem dokumentierten Wissen ebenso wie dessen mangelnde Verfügbarkeit entstehen (Alberts, Dorofee 2003, 95; Loomans 2004, 44). Demzufolge können aus einer entscheidungsorientierten Perspektive Fehlentscheidungen das Resultat der Nutzung von Wissen mangelnder Qualität sein (Coleman, Casselman 2004, 5, 12ff). Bezieht man die Problematik mit ein, dass die Durchführung von Geschäftsprozessen in vielen Fällen stark von IT-Systemen abhängig ist, so ergeben sich dadurch weitere Risiken, die in der Form von Engpässen zu einer Einschränkung der Qualität führen (Hirschmann, Romeike 2004, 13; Belsis et al. 2005, 189). Abhängigkeiten sind im Falle von dokumentiertem Wissen von besonderer Relevanz, da in IT-Systemen verwaltetes bzw. gesichertes Wissen zur Durchführung von Prozessen oder Aufgaben erforderlich ist und somit die Nichtverfügbarkeit der IT-Systeme die Prozesse der Wissensarbeit hemmen kann. Über dokumentiertes Wissen hinausgehend betreffen Abhängigkeiten auch die Kompetenzen bzw. Erfahrungen der Mitarbeiter, die bei mangelnder Verbreitung bzw. Redundanz zu Engpässen führen können und dadurch ebenfalls die Durchführung der Prozesse bzw. Aufgaben gehemmt werden kann (Kobi 1999, 13).

Bei einigen Ansätzen zum IT-RM (siehe Kapitel 4) stehen Ressourcen, die von den Risiken betroffen sind, im Mittelpunkt der Betrachtung. Dies setzt die Identifikation von potentiell risikobehafteten Ressourcen, deren Wertbestimmung und eine daraus resultierende Klassifikation des Schutzbedarfes voraus, wobei insbesondere bei immateriellen Ressourcen die Bewertung schwer ist und zudem Interdependenzen zwischen den Ressourcen zu beachten sind (Alberts, Dorofee 2003, 95; Bitkom 2003, 16; Suh, Han 2003, 150ff). Auch Ansätze zum Schutz vor Industriespionage bzw. Competitive Intelligence weisen zum Teil ein ressourcenfokussiertes Vorgehen auf (Lux, Peske 2002, 156). Dieser Stellenwert der Ressourcen wird auch dem Konzept Wissensrisiko zugrunde gelegt und somit davon ausgegangen, dass die verschiedenen Ursachen von Wissensrisiken wissensbezogene Ressourcen betreffen (siehe Abschnitt 2.2.3).

Bei der Auseinandersetzung mit Wissensrisiken ist zu beachten, dass sich diese ebenso wie auch traditionelle Risiken in ihrem strategischen Gehalt unterscheiden. Dies bedeutet, dass Wissensrisiken sowohl auf der strategischen als auch auf der operativen Unternehmensebene verursacht werden können bzw. sich auf diesen Ebenen auswirken können. Für die Steuerung von Risiken im Allgemeinen und Wissensrisiken im Speziellen ist jedoch eine Bewertung bzw. ein klares Verständnis des Risikos erforderlich. Dabei wird die Bewertung bzw. die Analyse von Ursachen und Wirkungen mit zunehmendem strategischen Gehalt erschwert, da die zu beachtenden Einflussfaktoren zunehmen und auch die Auswirkungen oftmals einen langfristigeren Charakter haben. Aus diesem Grund sind auf der strategi-

schen Ebene oftmals nur qualitative Bewertungen von Risiken möglich[138]. Aufgrund der geringeren Abstraktionsebene können die Auswirkungen von Wissensrisiken in den Bereichen Zeit, Kosten und Qualität (z.B. erhöhte Durchlaufzeiten, Ersatzkosten, mangelnde Nutzbarkeit) sowie deren Ursachen auf der Ebene der operativen Geschäftsprozesse den Fokus der Betrachtung bilden. Somit ist der hier vertretene Wissensrisikobegriff ebenso wie der operationelle Risikobegriff nach Basel II (siehe Abschnitt 3.3) auf die operative Unternehmensebene fokussiert und kann vielmehr als ein Teilausschnitt dieser Risikoauffassung verstanden werden.

Wie auch bereits bei der allgemeinen Diskussion von Risiken dargestellt (siehe Abschnitt 3.1), stellen die Risikobegriffe entweder auf die Ursachen oder die Wirkungen des Risikos ab, wobei sich diese beiden Elemente nicht ausschließen, sondern vielmehr integriert betrachtet werden können (Schulte 1997, 12; Bitz 2000, 13). Dieser Sichtweise wird auch hier gefolgt und somit eine zweistufige Wissensrisikodefinition zugrunde gelegt. Für die vier zuvor dargestellten Ursachen können die zwei Auswirkungen Mangel und Nichtexklusivität der wissensbezogenen Ressourcen definiert werden. Ein Mangel kann sich dabei auf Zeit, Kosten und Qualität[139] der Geschäftsprozessdurchführung auswirken, was mit finanziellen Verlusten verbunden sein kann. Nichtexklusivität als Auswirkung basiert auf der zentralen Annahme des ressourcenbasierten Ansatzes (siehe Abschnitt 2.1.1), dass Kernkompetenzen als Bündel von Ressourcen zum Aufbau bzw. zur dauerhaften Erhaltung von Wettbewerbsvorteilen die Eigenschaften wertvoll, knapp, nicht bzw. eingeschränkt imitierbar, nicht substituierbar sowie begrenzt abnutzbar, mobil und aneigenbar aufweisen müssen (Prahalad, Hamel 1990, 83ff; Barney 1991, 106f; Grant 1991, 123ff).

Bei wissensbezogenen Ressourcen ist aufgrund ihres immateriellen Charakters und der damit verbundenen vergleichsweise hohen Mobilität die Wahrung der Exklusivität entscheidend, um den Wert der wissensbezogenen Ressourcen und der darauf basierenden wissensbasierten Wettbewerbsvorteile zu erhalten (Norman 2002, 178; Jordan, Lowe 2004, 243). Durch eine Diffusion, also eine unerwünschte Kenntnisnahme durch nicht autorisierte Dritte, kann deren Wert gemindert werden oder sogar gänzlich verloren gehen. Besonders evident ist der Verlust der Exklusivität im Falle der Produktpiraterie, bei der durch den Einsatz von Reverse Engineering Aktivitäten Wissen aus Produkten destilliert wird. Auf diese Weise können Wettbewerbsvorsprünge, die auf überlegenem Wissen basieren, verloren gehen (Wildemann 2007, 37).

Generell können wie auch bei Risiken im Allgemeinen die finanziellen Verluste, die sich ergeben, näher spezifiziert werden. So kann beispielsweise wie bereits in Abschnitt 3.5.3 dargestellt, eine generische Unterteilung in monetär, qualitativ und reputationsbezogen vorgenommen werden (Gleißner

[138] Siehe hierzu auch Abschnitt 3.5.3.

[139] Den drei Kriterien Zeit, Kosten und Qualität kommt im Geschäftsprozessmanagement im Hinblick auf die Erbringung der Wertschöpfung eine bedeutende Rolle zu (Gaitanides et al. 1994, 3). Aufgrund der geschäftsprozessorientierten Ausrichtung gelten diese Kriterien auch für das Management von Wissensrisiken.

2001, 113; Mott 2001, 205; van den Brink 2001, 4; Seibold 2006, 19). Besser geeignet sind im Kontext von Wissensrisiken Kennzahlen, die dem immateriellen Charakter wissensbezogener Ressourcen Rechnung tragen. Dies trifft auf die Balanced Sorecard zu, die im Rahmen der wertorientierten Unternehmensführung entwickelt wurde und neben rein finanziellen Kennzahlen auch qualitative Kennzahlen einbezieht. Die Kennzahlen werden den vier Perspektiven Finanzen, Kunden, interne Prozesse sowie Lernen und Wachstum zugeordnet, wobei mittels perspektivenübergreifender Ursachen- und Wirkungsbeziehungen der Erfolg der Umsetzung der Unternehmensstrategie überprüft werden soll (Kaplan, Norton 1996, 9). Im Kontext des Managements von Wissensrisiken können sich die Risiken auf diese vier Perspektiven negativ auswirken und somit die Unternehmensentwicklung bzw. die Erreichung der Unternehmensziele hemmen. So können Wissensrisiken beispielsweise die Reduktion des Umsatzes durch imitierende Konkurrenten (Finanzen), mangelnde Kundenzufriedenheit aufgrund der Veröffentlichung sensitiver Inhalte (Kunden), eine Hemmung der Durchführung der Prozesse aufgrund eines Mangels an Kompetenzen (interne Prozesse) oder eine eingeschränkte Mitarbeiterzufriedenheit aufgrund hoher Fluktuation (Lernen und Wachstum) betreffen.

Geht man davon aus, dass Wissensrisiken insbesondere auf der operativen Ebene auftreten und sich durch ihre Aggregation auf die Wissensrisikoposition des Unternehmens auswirken können, so stellen die operativen Geschäftsprozesse einen geeigneten Analyserahmen für Wissensrisiken dar. Dennoch ist es bedeutend, auch Wissensrisiken auf der strategischen Ebene zu beachten, für diese Risiken zu sensibilisieren und so das Bewusstsein für Wissensrisiken zu erhöhen, wobei eine detaillierte Analyse aufgrund der genannten Gründe schwer zu operationalisieren ist. Basierend auf diesen Vorüberlegungen wird das Konzept Wissensrisiko wie folgt definiert.

Wissensrisiko ist ein operationelles Risiko, das (1) durch einen Verlust, (2) eine unerwünschte Diffusion, (3) einen unzureichenden Transfer oder (4) eine eingeschränkte Qualität von wissensbezogenen Ressourcen verursacht wird und in einem Mangel bzw. in einer Nichtexklusivität dieser Ressourcen resultiert.

Dabei weist die Definition folgende Besonderheiten auf. Wissensrisiken werden als Teil der operationellen Risiken[140] verstanden und sind somit auf die Ebene der operativen Geschäftsprozesse fokussiert. Die Definition folgt somit der Ausrichtung von Lindstaedt et al. (2004). Im Hinblick auf deren Management wird dabei vermutet, dass sie aufgrund ihrer geringeren Komplexität und kurzfristigen Wirkung vergleichsweise einfacher identifizierbar, bewertbar und steuerbar sind.

In Anlehnung an die Risikobetrachtung im IT-RM[141] ist es aufgrund des immateriellen Charakters von Informationen erforderlich, genau zu definieren, welche Ressourcen betroffen sind, um eine effiziente Steuerung vornehmen zu können. Diese Anforderung ist auch auf Wissensrisiken übertragbar, wobei

[140] Siehe hierzu Abschnitt 3.3.
[141] Siehe hierzu Kapitel 4.

zu beachten ist, dass diese Anforderung aufgrund des starken Personenbezugs von Wissen und dessen zum Teil impliziten Charakters vergleichsweise schwerer zu erfüllen ist. Demnach stellen die wissensbezogenen Ressourcen, die analog zu Ressourcen im IT-RM für die Ermittlung des Schutzbedarfes zu identifizieren und zu bewerten sind, im Fokus der Wissensrisikobetrachtung.
Zudem weist die Definition einen zweistufigen Charakter auf. Demzufolge werden die Risikoursachen Verlust, unerwünschte Diffusion, unzureichender Transfer und eingeschränkte Qualität den Wirkungen Mangel und Nichtexklusivität gegenübergestellt.
Nachdem die verschiedenen Teilkonzepte dargestellt wurden, erfolgt im folgenden Abschnitt eine integrierte Betrachtung der verschiedenen Ursachen operationeller Risiken im Allgemeinen und Wissensrisiken im Speziellen. Zudem werden die betroffenen wissensbezogenen Ressourcen zu diesen Ursachen in Bezug gesetzt und die daraus resultierenden Wirkungen erörtert. Diese Systematisierung stellt zugleich die Basis für die Analyse der konkreten Wissensrisiken zu den vier zentralen Konzepten in den Abschnitten 5.3-5.6 dar.

5.2 Systematisierung von Wissensrisiken

Nachdem die vier Teilkonzepte betrachtet wurden erfolgt deren Einordnung in den Gesamtzusammenhang. Zu diesem Zweck werden Ursache-Wirkungsbeziehungen herangezogen. Mittels der nachfolgenden Abb. 21 werden die bisherigen Überlegungen zu Wissensrisiken integriert und systematisiert. Wissensrisiken werden in diesem Kontext als Unterkategorie der operationellen Risiken verstanden. Operationelle Risiken werden wie in Abschnitt 3.3 dargestellt den vier Ursachenkategorien Personen, Prozesse, Systeme oder externe Faktoren sowie Kombinationen aus diesen zugeordnet (Basel 2004, 157). Die Kategorie Personen schließt alle Ursachen ein, die primär auf das Verhalten der Mitarbeiter zurückzuführen sind. Dabei können die Handlungen sowohl bewusst als auch unbewusst vorgenommen werden und auch durch Fahrlässigkeit charakterisiert werden. Auch mangelnde Kompetenzen der Mitarbeiter werden unter dieser Kategorie subsumiert (Kuhn 2002, 157; Piaz 2002, 57). Ursachen der zweiten Kategorie betreffen alle Risiken, die im primären Zusammenhang mit Schwächen der Prozesse oder sonstiger organisatorischer Richtlinien bzw. Verfahrensweisen stehen. Dies kann beispielsweise die unvollständige bzw. mangelhafte Definition der Prozesse sowie inkonsistente Rollendefinitionen betreffen (Seibold 2006, 18). Die Ursachenkategorie Systeme betrifft allgemein die IT des Unternehmens und im Speziellen Hardware, Software, Daten und Modelle (Piaz 2002, 57). Diese drei Kategorien subsumieren intern verursachte Risiken. Extern verursachte Risiken sind Gegenstand der Kategorie externe Faktoren.

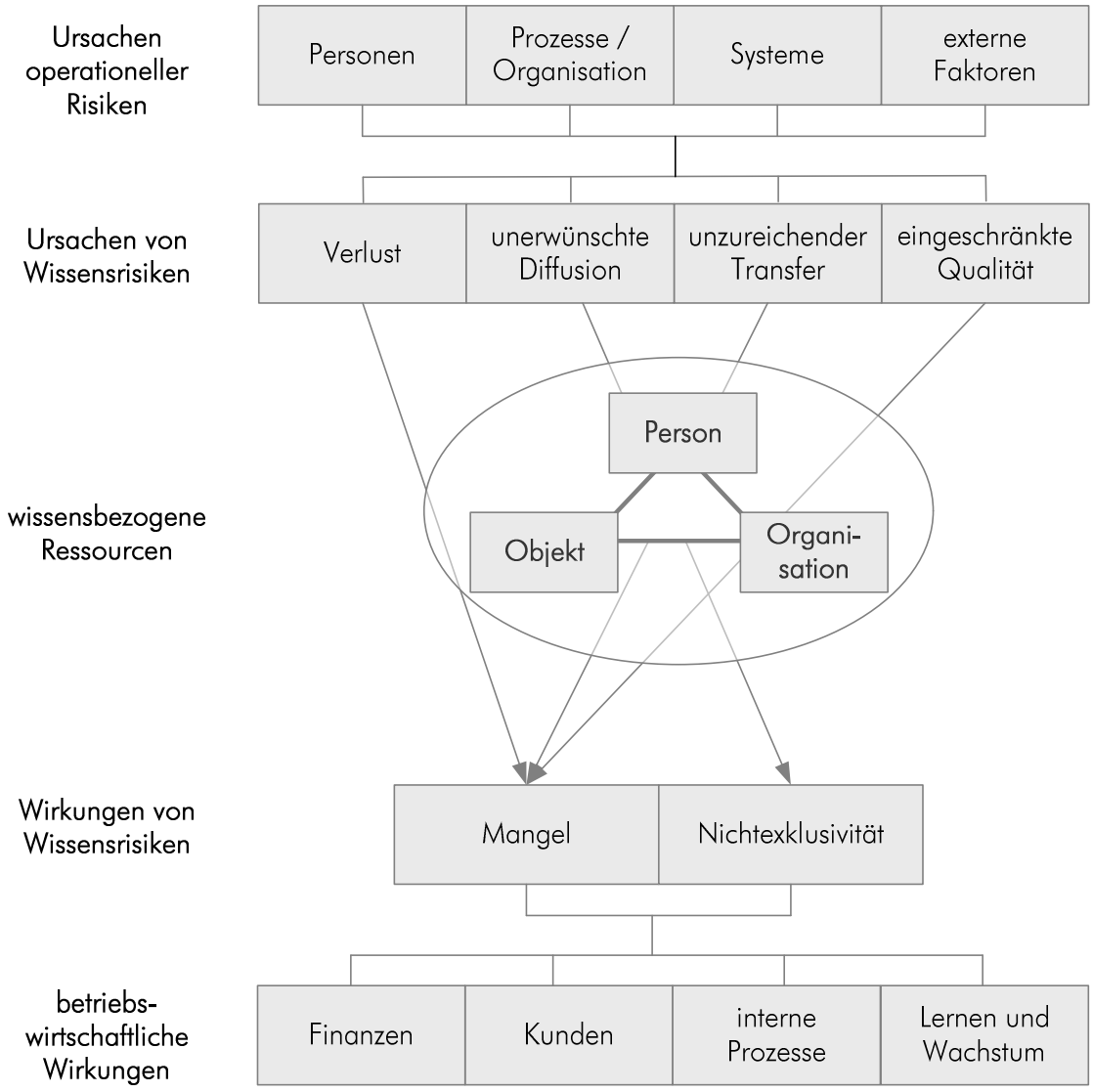


Abb. 21 Ursachen und Wirkungen von Wissensrisiken

Diese umfassen die Handlungen verschiedener externer Akteure wie Konkurrenten oder Hacker sowie Regulation und Katastrophen im Sinne höherer Gewalt (Piaz 2002, 57). Dabei sind Risiken vielfach nicht nur einer Kategorie zuordenbar, sondern betreffen zum Teil zwei oder mehr Kategorien, da sich Risiken auch aus dem Zusammentreffen verschiedener Ereignisse ergeben. Dies ist besonders evident im Bereich des IT-RM, da Angriffe als externe Faktoren Schwachstellen von Systemen als interne Faktoren voraussetzen. Auch die fahrlässige Weitergabe von sensitiven Inhalten, die auf eine Aushorchungsmaßnahme eines Konkurrenten zurückzuführen ist, verbindet zwei Kategorien. Dennoch kann den verschiedenen Risiken in der Regel eine primäre Ursache zugeordnet werden. So steht z.B. menschliches Fehlverhalten, das technische Versagen eines Systems oder eine Naturkatastrophe im Vordergrund. Da Personen vielfach das Auftreten eines Risikos beeinflussen, ist diese Kategorie für eine Vielzahl an Risiken von Relevanz. Dadurch wird die für eine Systematisierung erforderliche

Trennschärfe erschwert. Diese kann durch eine primäre Ursachenzuordnung gewährleistet werden. Dies bedeutet, dass eine primäre Ursache zugewiesen wird, auch wenn mehrere Risikokategorien betroffen sind. Somit werden der Kategorie Personen nur diejenigen Risiken zugeordnet, die direkt z.B. durch menschliches Versagen oder kriminelle Handlungen verursacht werden (Seibold 2006, 16).
Diese generischen Ursachenkategorien operationeller Risiken können im Hinblick auf Wissensrisiken durch die spezifischen Ursachen Verlust, unerwünschte Diffusion, unzureichender Transfer und eingeschränkte Qualität (siehe 5.3 bis 5.6) spezifiziert werden. Diese betreffen wissensbezogene Ressourcen, also personengebundenes, in Objekten inkorporiertes und organisatorisch verankertes Wissen. Dabei betrifft nicht jede Wissensrisikoursache jede Kategorie wissensbezogener Ressourcen. Die sich auf wissensbezogene Ressourcen auswirkenden Wissensrisikoursachen ziehen als Auswirkungen einen Mangel oder eine Nichtexklusivität dieser Ressourcen nach sich. Dabei wird die Wissensrisikowirkung Nichtexklusivität durch die Ursache Diffusion hervorgerufen und kann auch im Rahmen eines Verlustes auftreten, wenn beispielsweise Mitarbeiter, die zu anderen Unternehmen abgewandert sind, unternehmensspezifisches Wissen, wie z.B. Verfahrensanweisungen oder Prozessbeschreibungen, anwenden bzw. transferieren. Nach einem betriebswirtschaftlichen Risikoverständnis gehen Risiken mit Verlusten bzw. Schäden einher. Diese können sich auf unterschiedlichen Managementebenen auswirken. So können auf der Ebene der operativen Geschäftsprozesse Mängel an wissensbezogenen Ressourcen die Zeit, Kosten und Qualität der Geschäftsprozessdurchführung negativ beeinträchtigen. Generell können Risiken auf der Ebene der Geschäftsprozesse zu Mehraufwänden oder Mindererträgen führen. Die durch die Diffusion von sensitiven Inhalten verursachte Nichtexklusivität wissensbezogener Ressourcen kann die strategische Positionierung oder die Produktentwicklungsstrategie des Unternehmens negativ beeinträchtigen[142]. Als weitere Auswirkungen von Wissensrisiken auf der Unternehmensebene können negative Zielabweichungen, Opportunitätskosten, reduziertes Wachstum, Wertverluste des intellektuellen Kapitals oder Reputationsverluste angeführt werden (Klomfass, Quadt 2001, 322ff; Queensland 2001, 17; Salmela 2003, 3; Loomans 2004, 48). Wie in 5.1 ausgeführt, können die Auswirkungen von Wissensrisiken den vier Perspektiven Finanzen, Kunden, interne Prozesse sowie Lernen und Wachstum der Balanced Scorecard zugeordnet werden (Kaplan, Norton 1996, 9). In diesem Zusammenhang sind auch insbesondere kumulative Wirkungen von Risiken sowie Folgeschäden im Sinne von Wirkungsketten von Relevanz.
Betrachtet man die in Abb. 21 dargestellten Zusammenhänge anhand des konkreten Beispiels der Abwerbung eines qualifizierten Mitarbeiters durch einen Konkurrenten, so sind folgende Dimensionen betroffen. Die Abwerbung stellt im Hinblick auf die Ursachenkategorien einen externen Faktor

[142] So kann beispielsweise die Diffusion eines Konzeptes für ein neues Produkt an einen Konkurrenten eine Veränderung der Produktstrategie erforderlich machen und so zu Umsatzeinbußen führen oder durch die Diffusion und die daraus resultierende Verminderung des Technologievorsprungs die potentiellen Einnahmen von Nachfolgeprodukten reduzieren (Lux, Peske 2002, 104).

dar, da sie von einem Konkurrenten ausgeht. In Bezug auf die Ursachen von Wissensrisiken ist primär das Konzept Wissensverlust betroffen, da die Kompetenzen des Mitarbeiters dem Unternehmen fehlen. Als wissensbezogene Ressource ist die Kategorie Personen betroffen, da es sich um Mitarbeiterkompetenzen handelt. Ein derartiger Verlust resultiert gemäß der Definition in einem Mangel, der sich in Bezug auf die Perspektiven der Balanced Scorecard negativ auf die Durchführung der internen Prozesse auswirken kann. Weiterhin kann die Fluktuation des Mitarbeiters auch die Zufriedenheit der anderen Mitarbeiter senken oder auch den Verlust an Kunden zur Folge haben, wenn die Kundenbeziehungen stark personenbezogen sind. Weiterhin kann im Zuge dieses Unternehmenswechsels auch die Ursachenkategorie Wissensdiffusion betroffen sein, wenn der ehemalige Mitarbeiter Wissen beim Konkurrenten anwendet. Dies hätte weiterhin eine Einschränkung der Exklusivität zur Folge und könnte weitere Kennzahlen der vier Perspektiven, wie z.B. Umsatzrückgang durch Produktimitation, betreffen.

Durch das in Abb. 21 dargestellte Raster zu Ursachen und Wirkungen von Wissensrisiken lassen sich diese systematisieren. So können Wissensrisiken verschiedene Ursachenkategorien operationeller Risiken zugeordnet werden sowie einer spezifischen Wissensrisikoursache. Eine nähere Detaillierung ergibt sich zudem durch die betroffenen wissensbezogenen Ressourcen und den daraus resultierenden Wirkungen von Wissensrisiken. Diese können unterschiedliche Managementebenen betreffen und sich auf die Geschäftsprozessdurchführung selbst und / oder die Unternehmensebene auswirken.

Nachfolgende Abschnitte haben zum Ziel, diese Teilkonzepte detailliert zu betrachten und die in der Literatur identifizierten Wissensrisiken entsprechend der in diesem Abschnitt erarbeiteten Systematisierung zu konkretisieren. Als Primärgliederung werden zu diesem Zweck die Teilkonzepte Wissensverlust (5.3), Wissensdiffusion (5.4), Wissenstransfer (5.5) und Wissensqualität (5.6) von wissensbezogenen Ressourcen herangezogen. Die Auswirkungen Mangel und Nichtexklusivität folgen, wie erwähnt und in Abb. 21 dargestellt, unmittelbar diesen Ursachen. Sekundär werden die Wissensrisiken nach den betroffenen generischen Ursachenkategorien Personen, Prozesse, Systeme und externe Faktoren gegliedert, wobei eine trennscharfe Zuordnung auf die beiden Strukturierungsebenen durch das Kriterium der primären Ursachenzuordnung gewährleistet werden soll. Die Ableitung der Einzelrisiken basiert auf der Literatur, wobei verschiedene Forschungsfelder wie RM, Projekt-RM, IT-RM, Wirtschaftskriminalität, strategische Allianzen etc. einbezogen wurden. Neben der Betrachtung der Einzelrisiken werden je Konzept auch beispielhaft Interaktionen zwischen den Einzelrisiken analysiert, die ebenfalls auf der Literatur basieren. Dadurch sollen erste Anhaltspunkte gewonnen werden, welche Interaktionen bei der Steuerung besonders betrachtet werden sollten. Darüber hinaus werden in Abschnitt 5.7 konzeptübergreifende Interaktionen hoch aggregiert betrachtet, bevor in Abschnitt 5.8 die zentralen Ergebnisse dieses Abschnitts zusammengefasst werden.

5.3 Wissensverlust

Im nachfolgenden Abschnitt werden nach einer allgemeinen Betrachtung des Konzeptes Wissensverlust die in der Literatur identifizierten Einzelrisiken betrachtet.

5.3.1 Allgemeine Betrachtung

Ein Verlust an Wissen hat zur Folge, dass das Wissen dem Unternehmen dauerhaft nicht mehr zur Verfügung steht. Wie bereits in Abschnitt 5.1 dargestellt, können Wissensverluste regulär, also bewusst durch die Unternehmensleitung wahrgenommen werden und auch erwünscht sein. Dies betrifft z.B. die Kündigung von Mitarbeitern durch die Unternehmensleitung. Andererseits bestehen irreguläre Wissensverluste, die der Unternehmensleitung nicht bewusst oder nicht in ihrem Interesse sind (Liman 1999, 41ff; Mohamed et al. 2006, 3ff). Diese Art von Wissensverlusten bildet den Kern der nachfolgenden Betrachtungen, wobei folgendes Begriffsverständnis zugrunde gelegt wird.

Ein Wissensverlust bezeichnet einen Zustand, der durch Fluktuation, unzureichende Zusammenarbeit, Vernichtung bzw. Löschung sowie Nichtdokumentation verursacht wird und zur Folge hat, dass dem Unternehmen wissensbezogene Ressourcen dauerhaft nicht mehr zur Verfügung stehen.

Im Hinblick auf an Personen gebundenes Wissen[143] entstehen Wissensverluste vorwiegend durch die Fluktuation von Mitarbeitern (siehe auch Abb. 22)[144]. Primär wahrgenommen werden dabei die Extrafluktuation[145], also das Ausscheiden aus dem Berufsleben und Interfluktuation[146], die den Wechsel zu anderen Unternehmen betrifft. Auch die Intrafluktuation, die die Fluktuation innerhalb des Unterneh-

[143] Der mit der Fluktuation von Mitarbeitern einhergehende Verlust von Wissen wird auch als Brain Drain bezeichnet und stellt einen Verlust an intellektuellem Kapital dar, da Kompetenzen der Mitarbeiter verloren gehen bzw. nicht mehr zur Verfügung stehen (Elsner 2002, 18).

[144] Bestimmte Branchen oder Unternehmen sind dabei besonders durch Fluktuation bedroht. So werden bei der NASA in den nächsten Jahren mehr als 60% der Wissenschaftler in den Ruhestand eintreten. Daher werden intensive Anstrengungen unternommen, neue Mitarbeiter zu akquirieren und diese entsprechend anzulernen, um so die Wissensverluste zu kompensieren (Desouza, Awazu 2006, 32). Andere Unternehmen bzw. Branchen haben ähnliche Quoten, weisen aber zusätzlich das Problem auf, dass sie über ein geringes akquisitorisches Potential verfügen und somit neue Mitarbeiter nur schwer angeworben werden können. Dies betrifft beispielsweise die Formenbau- und Werkzeugindustrie (Mohamed et al. 2006, 3).

[145] Extrafluktuation wird u.a. durch Pensionierung, Vorruhestand, Altersteilzeit, Elternzeit, Berufsunfähigkeit und Tod des Mitarbeiters verursacht (Kiechle 2001, 19).

[146] Die Interfluktuation kann beispielsweise durch Dritte ausgelöst werden und mit Abwerbungsversuchen einhergehen. Zudem kann sie durch die Unternehmensleitung initiiert sein und z.B. auf einer Rationalisierungs- oder Restrukturierungsmaßnahme beruhen. Die Interfluktuation kann aber auch eigenmotiviert sein und beispielsweise auf mangelnde Karriereperspektiven, bessere Verdienstmöglichkeiten, Differenzen mit dem Arbeitgeber oder Kollegen oder den Wunsch nach Selbständigkeit zurückgeführt werden (Sabathil 1977, 15ff). Dabei können insbesondere auch Wettbewerbsdruck und Krisen dazu führen, dass qualifizierte Mitarbeiter das Unternehmen verlassen (Civi 2000, 171; Rosenblatt, Sheaffer 2001, 409f).

mens bezeichnet, kann Wissensverluste verursachen, wobei abgrenzend zu den anderen Typen die Mitarbeiter noch im Unternehmen vorhanden sind (Sabathil 1977, 13ff).

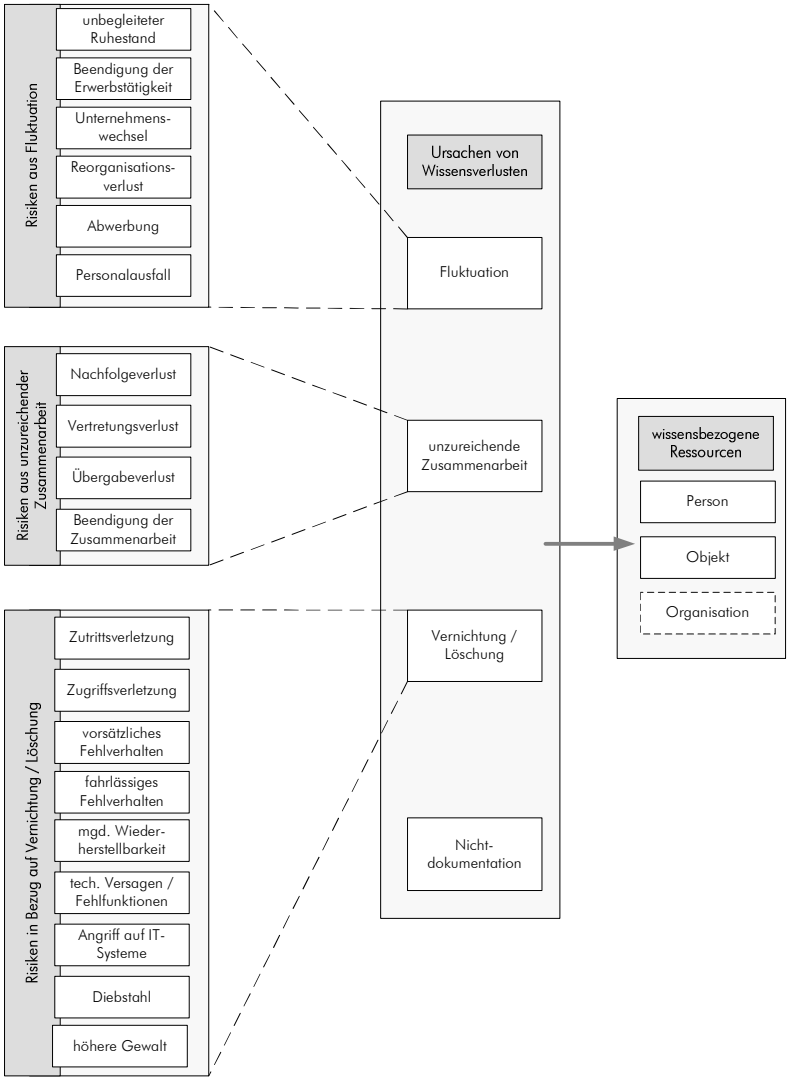


Abb. 22 Wissensrisiken im Kontext des Wissensverlustes

Während die Extrafluktuation vielfach außerhalb des Einflussbereiches des Unternehmens liegt, werden die anderen Formen der Fluktuation u.a. durch eine Reihe von Faktoren ausgelöst, die im Einflussbereich des Unternehmens liegen. Neben extern verursachten Abwerbungen und der Eigenmotivation der Mitarbeiter werden fluktuationsbedingte Wissensverluste insbesondere durch Reorganisationen, Fusionen und Übernahmen sowie die Projektorganisation, die vielfach in Unternehmen die Aufbauorganisation ergänzt, hervorgerufen. So werden Reorganisationen von Teams, Abteilungen, Geschäftsbereichen und Standorten vorgenommen und Prozessabläufe einem Reeingeneering unterzogen (Knaese 2004, 52). Auch im Zuge von Übernahmen oder Fusionen kann es im Rahmen des Abbaus von Doppelfunktionen zu Personaleinsparung und somit zu fluktuationsbedingten Wissensverlusten kommen (Probst, Knaese 1999, 13). Darüber hinaus zieht die Fluktuation noch weitere Folgerisiken im Sinne von Wissensverlusten nach sich, die bezogen auf das Modell zum intellektuellen Kapital (siehe Abschnitt 2.3.1) Beziehungskapital und Prozesskapital betreffen (Williams 2004, 371).

- **Verlust von Beziehungskapital**: Im Zuge der Fluktuation von Mitarbeitern kann neben Mitarbeiterkompetenzen auch Wissen über Kunden und Kundenbeziehungen verloren gehen. Auf diese Weise kommt es bzgl. des intellektuellen Kapitals zu einer Minderung des Kundenkapitals (siehe Abschnitt 2.3.1). Der Erwartungswert derartiger Verluste ist dann höher, wenn es sich um Mitar-

beiter mit ausgeprägtem Kundenverkehr (z.B. Berater mit eigenem Kundenstamm) handelt (van den Brink 2001, 65f; Knaese 2004, 43). Analoges gilt für Beziehungen zu anderen externen Stakeholdern, die von den fluktuierenden Mitarbeitern unterhalten wurden (Probst, Knaese 1999, 13; Williams 2004, 371).

- **Verlust von Prozesskapital**: Durch die Fluktuation von Mitarbeitern kann es auch zu einem Verlust von Prozesswissen kommen, da die Erfahrungen der Mitarbeiter in Bezug auf die Ausführung der entsprechenden Prozesse verloren gehen (van den Brink 2001, 66). Neben dem Verlust an Prozesswissen, das vergleichsweise besser formalisiert werden kann, geht mit der Fluktuation von Mitarbeitern auch der Verlust von Wissen über die Ausführung bestimmter wissensintensiver Routinen verloren. Diese sind weniger formalisierbar, basieren auf den Erfahrungen der Mitarbeiter und sind daher zu einem großen Anteil impliziter Natur. Aus diesen Gründen sind derartige Verluste im Vergleich zu Prozesswissen schwerer zu kompensieren (Williams 2004, 371). Das Schadensausmaß dieses Risikos nimmt zu, wenn mehrere Wissensträger gleichzeitig das Unternehmen verlassen (z.B. im Zuge der Abwerbung einer Abteilung), da sich dann die Verluste kumulieren und eine Kompensation der Verluste durch andere an den Prozessen beteiligten Mitarbeitern erschwert wird. Da Prozesse und Routinen durch die Fluktuation von Mitarbeitern negativ beeinträchtigt werden, wirkt sich eine stärkere Einbindung der Mitarbeiter in diese schwerwiegender aus. Somit kann die Fluktuation auch negative Effekte auf organisatorisch verankertes Wissen haben und beispielsweise zur Hemmung von Prozessen führen (Matusik 2002b, 608; Treleaven, Sykes 2005, 361ff).

Aus einer finanziellen Perspektive fallen Ersatzkosten an, deren Höhe durch das aktuelle Fachkräfteangebot auf dem Arbeitsmarkt bestimmt wird. So sind für die Rekrutierung neuer Mitarbeiter Personalsuchkosten zu veranschlagen[147]. Diese Beschaffung kann kostenintensiv sein, wobei in einigen Fällen kein adäquater Ersatz möglich ist (Kobi 1999, 72f; Knaese, Probst 2001, 36). Trotz dieser negativen Auswirkungen, ist Fluktuation nicht immer als negativ zu betrachten, sofern sie moderat erfolgt, da auch externes Wissen in das Unternehmen integriert wird und so eine Erweiterung der Wissensbasis erreicht werden kann (Matusik 2002b, 608).

Zum Zweiten können Wissensverluste durch eine unzureichende Zusammenarbeit verursacht werden und beispielsweise dann auftreten, wenn Nachfolger Stellen übernehmen, andere Mitarbeiter vertreten werden oder Übergaben zwischen Team- oder Projektmitgliedern unzureichend erfolgen. Weiterhin können sich Wissensverluste auch dann ergeben, wenn Mitarbeiter von der Projektorganisation in die Aufbauorganisation reintegriert werden oder die Zusammenarbeit mit Partnern beendet wird, da dadurch Beziehungen zu anderen Mitarbeitern verloren gehen können (Schindler 2001, 68; Burghardt 2002, 91; Disterer 2002, 512; Schindler, Eppler 2003, 220) (siehe auch Abb. 22).

[147] Siehe hierzu (Drumm 2000, 317ff).

Weiterhin kann dokumentiertes Wissen vernichtet bzw. gelöscht werden. Dies kann durch Zutritts- oder Zugriffsverletzungen von Mitarbeitern und externen Akteuren verursacht werden. Weitere Ursachen stellen Angriffe auf IT-Systeme oder technisches Versagen dar. Zudem kann Fehlverhalten der Mitarbeiter eine Ursache darstellen und sich darin äußern, dass Mitarbeiter sensitive Inhalte versehentlich oder absichtlich löschen. Ebenso kann es im Rahmen von Einbrüchen zum Diebstahl von Hardware kommen. Dies betrifft insbesondere auch mobile Endgeräte wie Notebooks oder mobile Datenspeicher, da deren Verlust ein erhöhtes Risiko darstellt (Desouza, Awazu 2004; Freeman 2004, 6)[148].

Letztlich können Wissensverluste auch durch den Prozess des Vergessens eintreten und betreffen die Nichtdokumentation von Erfahrungen oder Ideen (siehe Abb. 22). Die Notwendigkeit einer effizienten Dokumentation ergibt sich auch dann, wenn die Fluktuation von Mitarbeitern absehbar ist. Im Rahmen der Projektarbeit ist dieses Problem zum Teil bewusst und es bestehen verschiedenste Methoden, um Wissen, das im Rahmen der Projektarbeit gewonnen wurde, zu dokumentieren und auch so für andere Organisationsmitglieder verfügbar zu machen. So können beispielsweise Erfahrungen zum Projekt im Rahmen von Gesprächsrunden oder in schriftlicher Form zu bestimmten Meilensteinen oder am Projektende mittels verschiedener Methoden erfasst werden (Disterer 2002, 517; Schindler, Eppler 2003, 221ff). Neben projektspezifischem Wissen kommt allerdings auch der Dokumentation von Wissen, das im Rahmen des Tagesgeschäfts generiert wurde, eine Bedeutung zu, um Wissensverluste zu verhindern.

Im Hinblick auf die verschiedenen wissensbezogenen Ressourcen (siehe Abschnitt 2.2.3) betreffen Wissensverluste primär an Personen gebundenes bzw. in Objekten inkorporiertes Wissen. Bezüglich organisatorisch verankertem Wissen sind Verluste von geringerer Eintrittswahrscheinlichkeit bzw. weisen ein geringeres Schadensausmaß auf, da Wissen auf mehrere Organisationsmitglieder verteilt ist und somit individuelle Verluste von anderen Organisationsmitgliedern kompensiert werden können. Im Falle der Abwanderung ganzer Abteilungen (z.B. durch Management Buy-Out) ist jedoch auch ein umfassender Verlust organisatorisch verankerten Wissens denkbar.

5.3.2 Einzelrisiken

Personen: Wissensrisiken der Ursachenkategorie Person werden unternehmensintern verursacht und gehen vom Verhalten bzw. von Handlungen von Personen aus. Im Einzelnen werden folgende Wissensrisiken dieser Kategorie zugewiesen.

[148] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, sind 62% der befragten IT-Manager (in Unternehmen zwischen 500 und 5000 Mitarbeitern) davon überzeugt, dass kritische Informationen, die außerhalb der Rechenzentren auf Fileservern, PCs oder mobilen Engeräten vorgehalten werden, adäquat gegen Verlust geschützt sind. Bei Unternehmen mit mehr als 5000 Mitarbeitern waren 68% der IT-Manager vom Schutz der Informationen überzeugt.

- **unbegleiteter Ruhestand (VP1)**: Wie bereits in Abschnitt 5.3.1 erläutert, bestehen vielfältige Ursachen für Fluktuation, die zur Folge haben, dass Mitarbeiter das Unternehmen verlassen und deren Kompetenzen und Erfahrungen dem Unternehmen nicht mehr zur Verfügung stehen. Eine Ursache ist das altersbedingte Ausscheiden aus dem Erwerbsleben. Der Eintritt in den Ruhestand in verschiedenen Formen wie Altersteilzeit oder Vorruhestand kann als reguläre Fluktuation gesehen werden (Sabathil 1977, 14; Knaese 2004, 42f). Das Risiko des Ruhestands ist darin zu sehen, dass das Ausscheiden der Mitarbeiter unbegleitet erfolgt.
- **Beendigung der Erwerbstätigkeit (VP2)**: Wissensverluste können zudem dadurch hervorgerufen werden, dass Mitarbeiter sich dazu entscheiden, permanent aus dem Erwerbsleben auszuscheiden. So kann beispielsweise eine Beendigung durch Kindererziehung und die Nichtinanspruchnahme des freigehaltenen Arbeitsplatzes verursacht werden. Ferner können sich Mitarbeiter aus weiteren persönlichen Gründen dazu entscheiden, sich vollkommen aus dem Erwerbsleben zurückzuziehen (Sabathil 1977, 14; Kiechle 2001, 19; Knaese 2004, 42f). Die Eintrittswahrscheinlichkeit dieses Risikos ist schwer zu ermitteln, da die Entscheidungen unter Umständen kurzfristig getroffen werden.
- **Unternehmenswechsel (VP3)**: Neben dem Ausscheiden aus dem Erwerbsleben kann sich ein Wissensrisiko dadurch ergeben, dass ein Mitarbeiter zu anderen Unternehmen oder im Speziellen zu einem Wettbewerber wechselt. Dies kann auf Eigenmotivation basieren, die beispielsweise auf Unzufriedenheit im Unternehmen, bessere Verdienst- oder Aufstiegsmöglichkeiten zurückgeführt werden kann (Sabathil 1977, 15ff)[149]. Die Interfluktuation und damit der Verlust von Kompetenzen kann ebenfalls dadurch hervorgerufen werden, dass sich Mitarbeiter selbständig machen bzw. ein eigenes Unternehmen ausgründen. Durch derartige Ausgründungen können zudem neue Konkurrenten erwachsen und somit Wissen zum Nachteil des Unternehmens eingesetzt werden. Analoges gilt für den Wechsel zu Konkurrenten (Liman 1999, 241).
- **fahrlässiges Fehlverhalten (VP4)**[150]**:** Wissensverluste können sich daraus ergeben, dass Mitarbeiter, die an sie gestellten Anforderungen im Hinblick auf den Umgang mit Wissen nicht erfüllen. Dies kann sich darin äußern, dass bestehende Richtlinien nicht beachtet werden oder Mitarbeiter sorglos mit Wissen umgehen (BSI 2006, 486, 532f). So können beispielsweise definierte IT-Sicherheitsrichtlinien oder Richtlinien zum Umgang mit sensitiven Inhalten nicht eingehalten werden und so elektronisch oder physisch dokumentiertes Wissen nicht entsprechend gesichert sein. Neben der Nichteinhaltung bestimmter Vorschriften kann sich Fehlverhalten von Mitarbeitern auch darauf beziehen, dass dokumentiertes Wissen versehentlich gelöscht wird (BSI 2006,

[149] Die Attraktivität des Unternehmens für die Mitarbeiter im Vergleich zu anderen Unternehmen wird als akquisitorisches Potential bezeichnet und schließt u.a. Vergütung, Art der Aufgaben, Aufstiegschancen ein (Drumm 2000, 335).

[150] Die Unterscheidung zwischen vorsätzlichem und fahrlässigem Fehlverhalten ist insbesondere im IT-RM weit verbreitet (siehe hierzu auch Kapitel 4).

485). Fahrlässigkeit kann auch darauf zurückgeführt werden, dass erforderliche Kompetenzen im Umgang mit sensitiven Inhalten im Allgemeinen oder IT-Systemen im Speziellen fehlen (Abell, Oxbow 2002, 128ff; BSI 2006, 491)[151].

- **vorsätzliches Fehlverhalten (VP5)**: Neben einem fahrlässigen Fehlverhalten der Mitarbeiter können diese sich auch vorsätzlich über definierte Richtlinien hinwegsetzen, um dem Unternehmen aus Eigeninitiative oder zu Gunsten eines Dritten zu schaden. So kann beispielsweise dokumentiertes Wissen vorsätzlich durch Mitarbeiter gelöscht bzw. vernichtet werden, um bestimmte Sachverhalte zu verzerren oder eigene Interessen durchzusetzen (Alter 2006, 3). Die mutwillige Zerstörung von Datenträgern oder Geräten sowie die Löschung von Inhalten kann auf verschiedene Ursachen wie Rache, Böswilligkeit oder Frustration zurückgeführt werden (BSI 2006, 671, 675).

Prozesse: Wissensverluste in Bezug auf die Kategorie Prozesse betreffen Ursachen, die mit Schwächen von Prozessen, organisatorischen Richtlinien bzw. Verfahrensweisen in Zusammenhang stehen bzw. gehen von verschiedenen Maßnahmen aus, die seitens des Unternehmens ergriffen wurden.

- **Reorganisationsverlust (VO1)**: Wissensverluste können durch Reorganisationsmaßnahmen verursacht werden, die ihrerseits mit Restrukturierungen, Fusionen oder Akquisitionen in Zusammenhang stehen und zur Folge haben, dass Mitarbeiter zu anderen Unternehmen wechseln, aus dem Erwerbsleben ausscheiden oder unternehmensintern neue Stellen besetzen. Dabei kann der vom Unternehmen verursachte Stellenabbau erwünscht sein oder durch verschiedene Faktoren, wie z.B. drohende Insolvenz oder Abbau von Doppelfunktionen bei Fusionen oder Übernahmen durch Dritte, erforderlich werden. Ein Abbau von Stellen wirkt sich negativ auf das intellektuelle Kapital des Unternehmens aus, da Wissensträger das Unternehmen verlassen, während durch Intrafluktuation die Transparenz über das vorhandene Wissen verloren gehen kann (Probst, Knaese 1999, 13; DeNisi et al. 2003, 17; Williams 2004, 368).
- **Nichtdokumentation (VO2):** Personengebundenes Wissen, wie z.B. Erfahrungen aus Projekten, kann über den Prozess des Vergessens verloren gehen. Werden Erfahrungen oder Ideen, die im Tagesgeschäft oder im Rahmen des Projektgeschäfts gemacht wurden, nicht dokumentiert, gehen sie verloren. Dabei ist die Dokumentation im Hinblick auf die Vermeidung von Doppelarbeiten und die Nutzung von Synergien von Bedeutung. So kann die Nichtnutzung von in anderen Projekten entwickeltem Wissen zusätzlichen Aufwand generieren oder zur Wiederholung von Fehlern führen oder zur Folge haben, dass Problemlösungsprozesse nicht verkürzt werden. Dies hat negative Auswirkungen auf die Durchführung der Prozesse. Auch von der mangelnden Erfassung von

[151] Ein derartiger Mangel an Kompetenzen kann in verschiedenen Varianten vorliegen. So können Mitarbeiter im Glauben alles richtig zu machen handeln, die fehlenden Kenntnisse nicht zugeben oder bestrebt sein, die Kompetenzlücken zu schließen (van den Brink 2001, 5).

Wissen über Kunden geht in diesem Kontext ein Risiko aus (Disterer 2002, 517; Schindler, Eppler 2003, 221ff; Desouza, Vanapalli 2005, 84; Probst et al. 2006, 74).

- **Nachfolgeverlust (VO3):** Wissensverluste können sich auch daraus ergeben, dass ein systematischer Wissenstransfer zwischen Vorgänger und Nachfolger unterbleibt oder dieser unzureichend ist. So kann die Qualität des Wissenstransfers bei Nachfolge v.a. durch Zeitdruck negativ beeinträchtigt werden (Rüstmann 1999, 214ff)[152]. Dieser ist insbesondere dann gegeben, wenn aufgrund einer kurzfristigen Fluktuation keine antizipative Vorbereitung möglich ist und die Nachbesetzung reaktiv erfolgen muss. Ist das zur Ausführung der Stelle bzw. der entsprechenden Aufgaben erforderliche Wissen nicht erfasst oder kann die Einarbeitung und Wissensvermittlung nicht durch andere Mitarbeiter erfolgen, können neben anfänglichen mit der Einarbeitung einhergehenden Performanceschwächen auch Wissensverluste schwer kompensiert werden.
- **Vertretungsverlust (VO4):** Ebenso wie bei der Nachfolge von Mitarbeitern kann auch im Rahmen einer Vertretung das zur Ausführung der Stelle bzw. Aufgaben erforderliche Wissen fehlen und somit ein Mangel entstehen. Vertretungen erfolgen im Vergleich zur Nachfolge temporär und sind somit nicht permanent. Geht man allerdings davon aus, dass sich Krankheiten von Mitarbeitern unter Umständen über Wochen und Monate erstrecken, kann Vertretung mit einer Nachfolge gleichgesetzt werden. Ein wesentlicher Unterschied besteht darin, dass Vertretungen im Vergleich zur Nachfolge vielfach kurzfristiger sind und aus diesen Gründen oftmals nur eine reaktive Planung möglich ist. Aufgrund der reaktiven Planung nimmt die Wahrscheinlichkeit von Fehlern bei der Durchführung der entsprechenden Aufgaben zu (van den Brink 2001, 66).
- **Übergabeverlust (VO5):** Neben der Nachfolge und Vertretung von Mitarbeitern können sich Wissensverluste über den Prozess des Vergessens auch aus einer unzureichenden Übergabe von z.B. Aufgaben oder Arbeitsfortschritten zwischen den Mitarbeitern ergeben. Verschiedene Arbeitssituationen wie Job Sharing oder Teamarbeit allgemein erfordern die Übergabe von Wissen zu bestimmten Arbeitsinhalten an andere Mitarbeiter. Sind die Übergabeprozesse nicht entsprechend definiert, kann es zu Reibungsverlusten kommen und das zur Ausführung bestimmter Aufgaben erforderliche Wissen verloren gehen (Pfitzer et al. 2002, 2006).
- **Zutrittsverletzung (VO6):** Die Eintrittswahrscheinlichkeit von Wissensverlusten wird zudem dadurch erhöht, dass Zutrittsrechte zu den Unternehmensgebäuden allgemein bzw. zu bestimmten Bereichen innerhalb des Unternehmensgeländes unzureichend im Sinne von zu freigebig definiert sind oder eine entsprechende Rechtevergabe fehlt. Neben der unzureichenden Definition von Rechten können Zutrittskontrollen unzureichend sein und somit die Einhaltung entsprechend definierter Rechte nicht durchgesetzt werden. Liegt ein unzureichendes Management der Zutrittsrech-

[152] Ein derartiger Verlust ist in der Regel nie vollständig zu vermeiden, da nicht das gesamte Wissen des Vorgängers auf den Nachfolger transferiert werden kann. Jedoch können Verluste bei einer proaktiven, langfristigen und systematischen Nachfolgeplanung abgeschwächt werden.

te vor, können unautorisierte unternehmensinterne und -externe Personen Kenntnis nehmen und sich dokumentiertes Wissen, Prototypen etc. aneignen (BSI 2006, 332).

- **Zugriffsverletzung (VO7):** Ebenso wie im Falle der Zutrittsrechte (siehe VO6) kann auch das Management der elektronischen Zugriffsrechte unzureichend sein. So kann einerseits die Definition der Zugriffsrechte zu freigebig bzw. umfassend erfolgen und andererseits die Durchsetzung der definierten Rechte nicht entsprechend erfolgen. Je umfassender und unkontrollierter der Zugriff auf sensitive Inhalte erfolgt, umso höher ist die Wahrscheinlichkeit, dass Wissensverluste auftreten (BSI 2006, 626)[153].
- **unbegleitete Beendigung der Zusammenarbeit (VO8):** Risiken in Bezug auf Wissensverluste können sich auch dann realisieren, wenn Beziehungen zu Kooperationspartnern, Lieferanten oder Kunden beendet werden bzw. diese gewechselt werden. Insbesondere durch langfristige Zusammenarbeit wird umfassendes kollektives Wissen aufgebaut. Bei einer unbegleiteten Beendigung der Beziehungen bzw. mit dem Wechsel kann einerseits Wissen verloren gehen und andererseits wie im Falle der Einarbeitung von neuen Mitarbeitern eine Reduktion der Leistungsfähigkeit einhergehen (Kronen 1994, 67; Wagner 2003, 99). Das Schadensausmaß derartiger Wissensverluste ist dann besonders gravierend, wenn die Kooperation als Substitut jegliche Eigenentwicklung von Wissen angesehen wird (Lei 1993, 37; Schwamborn 1994, 241). Neben einer geplanten und bewussten Beendigung der Zusammenarbeit kann auch ein unerwarteter Rückzug des Partners erfolgen, der außerhalb des Einflussbereiches des Unternehmens liegt.

Systeme: Wissensverluste, die der Ursachenkategorie Systeme zugeordnet werden, betreffen die Informationstechnologie des Unternehmens. Dabei werden nachfolgend insbesondere Risiken erörtert, die sich aus Versagen der Hardware, Fehlern der Software oder der Fehlkonfiguration der Systeme ergeben.

- **technisches Versagen / Fehlfunktionen (VS1)**: Wissensverluste können sich daraus ergeben, dass z.B. Systeme oder Speicherkomponenten aufgrund technischen Versagens nicht mehr nutzbar sind bzw. die gesicherten Inhalte nicht wieder rekonstruiert werden können (BSI 2006, 306). Auch temporäre Systemabstürze können den Verlust von dokumentiertem Wissen zur Folge haben. Diese können beispielsweise auch die Folge von Stromausfällen sein. Analoges gilt für Fehler der Anwendungssoftware, die z.B. zur Folge haben können, dass bestimmte Operationen nicht ausgeführt werden (Hadden, Hermanson 2003, 36; Knaese 2004, 39; BSI 2006, 590ff).
- **mangelnde Wiederherstellbarkeit (VS2)**: Wissensrisiken im Hinblick auf Wissensverluste können sich daraus ergeben, dass die Maßnahmen zur Datensicherung unzureichend sind, da so die durch verschiedene Ereignisse, wie z.B. Löschung, IT-Sicherheitsvorfälle oder technisches Versa-

[153] Für weitere Details zu Zugriffsrechten siehe Abschnitt (siehe hierzu Kapitel 4) oder die Risikodiskussion in Abschnitt 5.4, da die Zugriffsrechtevergabe primär Risiken im Kontext der Wissensdiffusion betreffen.

gen, bedingten Datenverluste nicht oder nur bedingt wieder herstellbar sind (Knaese 2004, 40; BSI 2006, 65ff). Neben den organisatorischen Verpflichtungen und der Einbindung der Mitarbeiter, die Gegenstand verschiedener organisatorischer Richtlinien sein können, ist aus der Perspektive der IT-Systeme die einwandfreie technische Umsetzung und die Zuverlässigkeit bedeutend. Dies schließt zudem eine Planung der Speicherkapazitäten ein, da bei erschöpften Speichermedien Datenverluste auftreten können. Ebenso Gegenstand ist eine entsprechende Lagerung von Backup-Medien, da durch die Verkettung mehrerer Risikoereignisse eine Rücksicherung über diese Medien erforderlich sein kann (Kruth 2004, 151; BSI 2006, 65ff, 609).

externe Faktoren: Neben internen Ursachen der Kategorien Personen, Prozesse und Systeme können Wissensverluste auch auf externe Faktoren zurückgeführt werden. Nachfolgend werden die dieser Kategorie zugeordneten Wissensrisiken erläutert.

- **Abwerbung (VE1)**: Neben der Eigenmotivation der Mitarbeiter oder Maßnahmen seitens des Unternehmens kann die Interfluktuation auch extern durch andere Unternehmen im Allgemeinen sowie Headhunter oder Konkurrenten im Speziellen verursacht werden, indem die Mitarbeiter gezielt abgeworben werden. Derartige Risiken betreffen insbesondere hoch qualifizierte Mitarbeiter, die Schlüsselpositionen im Unternehmen einnehmen bzw. über strategisch wertvolle Kompetenzen verfügen (Sabathil 1977, 15ff; Maier 1992, 43f; Staudt 1992, 126; Liman 1999, 240). Das Bekleiden von Schlüsselpositionen bzw. das Halten entsprechender Kompetenzen erhöht in diesem Fall das Schadensausmaß. Die Abwerbung durch Headhunter oder sonstige Dritte kann auch dadurch begünstigt werden, dass diese Kenntnis über betriebliche Expertiseverzeichnisse erlangen (Probst et al. 2006, 71). Dieses Risiko ergibt sich dabei durch die aus dem WM resultierende erhöhte Transparenz.
- **Personalausfall (VE2)**: Neben dem Ruhestand ergeben sich Risiken in Bezug auf Wissensverluste daraus, dass Mitarbeiter dem Unternehmen für einen bestimmten Zeitraum nicht zur Verfügung stehen. Dabei stellen einerseits Krankheiten[154] einen Grund für einen temporären bzw. längerfristigen Personalausfall dar. Zum anderen kann Berufsunfähigkeit des Mitarbeiters, die eventuell als Folge einer Krankheit auftreten kann, zu einem permanenten Personalausfall und zugleich einem Ausscheiden des Mitarbeiters aus dem Arbeitsmarkt führen. Analoges gilt für den Tod von Mitarbeitern (Sabathil 1977, 14f; Kiechle 2001, 19; Knaese 2004, 42f). Die Eintrittswahrscheinlichkeit derartiger langfristiger bzw. permanenter Wissensverluste ist schwer zu prognostizieren, da die bedingenden Ereignisse vielfach kurzfristig auftreten, weshalb zumeist nur eine reaktive Steuerung dieser Risiken möglich ist.

[154] Es wird in diesem Kontext keine Unterscheidung vorgenommen, ob die Krankheit auf ein Handeln bzw. Verschulden des Mitarbeiters zurückzuführen ist oder nicht, sondern eine generelle Ursachenzuordnung zu externen Faktoren unterstellt.

- **Diebstahl (VE3)**: Eine weitere Ursache für Wissensverluste stellt der Diebstahl von physisch oder elektronisch dokumentiertem Wissen dar. Derartige Verluste können im Zuge von Einbrüchen in Unternehmensgebäude und der entsprechenden Entwendung der Hardware, Datenträger oder physischen Dokumente erfolgen. Besonders bedroht sind in diesem Kontext auch mobile Endgeräte wie Notebooks oder PDAs oder mobile Datenspeicher (z.B. USB-Sticks[155]), die ebenso sensitive Inhalte enthalten können (Liman 1999, 238f; Desouza, Awazu 2004, 6; Freeman 2004, 6; BSI 2006, 648). Im Falle des Diebstahls von Notebooks, der jährlich ca. 6% aller Notebooks betrifft (Pohlmann 2006, 31), gehen vielfach die Arbeitsfortschritte ab der letzten Synchronisation bzw. der letzten wieder herstellbaren Datensicherung verloren. Wissensverluste können sich neben einem Diebstahl auch daraus ergeben, dass Dritte, die sich Zutritt verschafft haben, oder Mitarbeiter, die im Auftrag eines Dritten handeln IT-Systeme sabotieren, dokumentiertes Wissen löschen bzw. zerstören (BSI 2006, 779). Dabei schließt Diebstahl in diesem Kontext auch die unautorisierte Aneignung liegengelassener bzw. gefundener Objekte mit ein.
- **Angriff auf IT-Systeme (VE4)**: Wissensverluste in Bezug auf elektronisch dokumentiertes Wissen können auch die Folge von externen Angriffen auf die IT-Systeme des Unternehmens sein. Dabei kann eine Vielzahl an Angriffen, wie z.B. Denial of Service Attacken oder die Einschleusung von Viren oder Würmern, herangezogen werden, die zur Folge haben können, dass in IT-Systemen dokumentiertes Wissen aufgrund von Nichtnutzbarkeit oder Löschung verloren geht (Noufal 2003, 144; Knaese 2004, 39; Kruth 2004, 163).
- **höhere Gewalt (VE5)**: Neben gezielten externen Angriffen oder technischem Versagen von Systemen können Wissensverluste auch auf höhere Gewalt, wie z.B. Feuer-, Sturm-, Wasser- oder Blitzschäden, zurückgeführt werden (BSI 2006, 304ff). Eine entsprechende Prognose der Eintrittswahrscheinlichkeit derartiger Risiken ist durch die externe Bedingung schwer möglich[156].

Nach der Betrachtung der Einzelrisiken werden im nachfolgenden Abschnitt die Interaktionen zwischen den Einzelrisiken analysiert.

[155] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, sehen 68% der befragten IT-Manager im Einsatz von USB Sticks zunehmend ein Risiko in Bezug auf den Verlust vertraulicher Inhalte oder deren Diffusion (Collins, Vile 2007, 3).

[156] Rückversicherer ermitteln allerdings die Eintrittswahrscheinlichkeit derartiger Schäden auf der Basis historischer Schadensdatenbanken und der regionalen Lage des Versicherten.

5.3.3 Diskussion

Die vorangegangenen Betrachtungen haben gezeigt, dass in den vier verschiedenen Kategorien Personen, Prozesse, Systeme und externe Faktoren jeweils Wissensrisiken bestehen (siehe Tab. 8). So sind in der Kategorie Personen zum einen Wissensrisiken im Kontext der Fluktuation von Relevanz. Weiterhin können Wissensverluste auch auf Fehlverhalten der Mitarbeiter zurückgehen. Hinsichtlich der Kategorie Prozesse können Wissensverluste auftreten, wenn Prozesse in den Bereichen Zusammenarbeit, Dokumentationspflichten sowie Gewährung von Zugang und Zugriff unzureichend definiert sind. Wissensverluste im Kontext von IT-Systemen gehen einerseits auf technisches Versagen bzw. Fehlfunktionen und andererseits auf die mangelnde Wiederherstellbarkeit von gelöschten Inhalten zurück. Wissensverluste der Kategorie externe Faktoren gehen u.a. auf Aktivitäten Dritter zurück und schließen dabei die Abwerbung von Mitarbeitern, Diebstahl oder Angriffe ein. Weiterhin sind dieser Kategorie auch Wissensverluste, die durch höhere Gewalt und Personalausfall verursacht werden, zuzuordnen.

Kategorie	No	Wissensrisiko
Personen	VP1	unbegleiteter Ruhestand
	VP2	Beendigung der Erwerbstätigkeit
	VP3	Unternehmenswechsel
	VP4	fahrlässiges Fehlverhalten
	VP5	vorsätzliches Fehlverhalten
Prozesse	VO1	Reorganisationsverlust
	VO2	Nichtdokumentation
	VO3	Nachfolgeverlust
	VO4	Vertretungsverlust
	VO5	Übergabeverlust
	VO6	Zutrittsverletzung
	VO7	Zugriffsverletzung
	VO8	unbegleitete Beendigung der Zusammenarbeit
Systeme	VS1	technisches Versagen / Fehlfunktionen
	VS2	mangelnde Wiederherstellbarkeit
externe Faktoren	VE1	Abwerbung
	VE2	Personalausfall
	VE3	Diebstahl
	VE4	Angriff auf IT-Systeme
	VE5	höhere Gewalt

Tab. 8 Wissensrisiken der Kategorie Wissensverlust

Wie im Kapitel Risiko- und RM bereits dargestellt[157], sind die Einzelrisiken nicht isoliert voneinander, da Interaktionen zwischen diesen bestehen und somit kumulative bzw. kompensierende Wirkungen auftreten können. Da der Untersuchungsgegenstand jedoch vergleichsweise jung ist, bestehen nur wenige Erkenntnisse zu potentiellen Interaktionen, die sich durch die bestehende Literatur absichern lassen. So wirken sich beispielsweise Wissensverluste, die aus der Fluktuation der Mitarbeiter resultieren, dann vergleichsweise schwerwiegender aus, wenn Dokumentationen zu den spezifischen Aufgaben des Mitarbeiters fehlen bzw. diese unzureichend sind, da so eine Kodifizierung des Wissens fehlt (Sanchez 1995, 7; Amelingmeyer 2002, 150ff). Weiterhin interagieren die Wissensrisiken im Kontext der Fluktuation mit der Definition von Nachfolge- und Vertreterregelungen. Sind diese Regelungen unzureichend definiert, ist das Schadensausmaß vergleichsweise höher, da dann neben dem eigentlichen Verlust der Mitarbeiterkompetenzen auch die Einarbeitung neuer Mitarbeiter erschwert

[157] Siehe hierzu Abschnitt 3.5.3.

wird. Diese ist insbesondere dann schwer, wenn sie kurzfristig bzw. reaktiv erfolgen muss (Knaese 2004, 43; Mohamed et al. 2006, 8). Darüber hinaus kann Fehlverhalten der Mitarbeiter im Umgang mit IT-Systemen und im Speziellen Sicherheitstechnologien zur Folge haben, dass die Erfolgswahrscheinlichkeit von Angriffen auf IT-Systeme ansteigt, da auf diese Weise erforderliche Schwachstellen geschaffen werden, die zu einem Verlust führen können (BSI 2006, 491).

Neben der Interaktion zwischen verschiedenen Einzelrisiken wird das Risikopotential im Bereich der Wissensverluste auch dadurch bestimmt, inwiefern Einzelrisiken mehrfach auftreten. So können beispielsweise mehrere Angriffe auf IT-Systeme, die Löschung von Inhalten oder die Fluktuation von Mitarbeitern simultan oder in geringem zeitlichen Abstand erfolgen und so die Gesamtrisikoposition erhöhen. Besonders evident ist dies im Falle der Fluktuation mehrerer Wissensträger, da dadurch die Kompensation der dadurch entstandenen Mängel erschwert wird. So können einerseits Kompetenzen, die auf mehrere Mitarbeiter verteilt sind bzw. von diesen gehalten werden, nicht mehr zur Verfügung stehen. Zudem kann eine stärkere Beeinträchtigung des Prozesswissens vorliegen, da bedingt durch die Anzahl der Fluktuationen das zur Ausführung der Prozesse bzw. Routinen erforderliche Wissen nicht verfügbar ist. Neben der Kumulation der einzelnen Fluktuationen kann ein derartiges Risiko auch durch die Abwerbung mehrerer Mitarbeiter bzw. ganzer Abteilungen erfolgen (Kobi 2003, 104).

Insgesamt bleibt im Hinblick auf das Schadensausmaß von Wissensverlusten festzuhalten, dass neben der redundanten Vorhaltung und der Wiederherstellbarkeit von dokumentiertem Wissen das Schadensausmaß auch dadurch beeinflusst wird, inwiefern vormals dokumentiertes Wissen durch Personen rekonstruiert werden kann. So kann beispielsweise ein gestohlener oder durch einen Brand vernichteter Konzeptentwurf durch den oder die Mitarbeiter, die das Konzept entworfen haben, rekonstruiert werden. Ist dies der Fall ist das Schadensausmaß des Wissensverlustes auch bei fehlender redundanter Vorhaltung oder mangelnder Wiederherstellbarkeit gering. Dieser Faktor ist somit bei der Bewertung sämtlicher Wissensverluste zu berücksichtigen und kann das Schadensausmaß limitieren.

5.4 Wissensdiffusion

Im Rahmen dieses Abschnittes werden ausgehend von einer allgemeinen Betrachtung Wissensrisiken, die mit der unerwünschten Diffusion von wissensbezogenen Ressourcen einhergehen, erörtert und dabei den vier Ursachenkategorien Personen, Prozesse, Systeme und externe Faktoren zugeordnet.

5.4.1 Allgemeine Betrachtung

Abgrenzend zum zuvor thematisierten Wissensverlust sind bei der unerwünschten Diffusion die wissensbezogenen Ressourcen noch vorhanden, aber nicht nur beim Unternehmen, sondern auch bei Dritten. Von der Risikoursache Diffusion, die die Verbreitung von sensitivem bzw. wettbewerbsrelevantem Wissen an nicht autorisierte unternehmensinterne und -externe Personen zum Gegenstand hat,

geht aus wettbewerbsorientierter Sicht ein besonders hohes Risiko aus, da es durch die Verbreitung zu einem Verlust an Exklusivität und somit zu einer Entwertung der wissensbezogenen Ressourcen kommen kann. Folglich kann das Konzept Wissensdiffusion folgendermaßen definiert werden.

Eine Wissensdiffusion bezeichnet den Zustand, in dem unautorisierte Personen aufgrund verschiedener extern oder intern bedingter Ereignisse von wissensbezogenen Ressourcen Kenntnis nehmen und dadurch deren Exklusivität gemindert wird.

Ausgehend vom ressourcenbasierten Ansatz (siehe Abschnitt 2.1.1), nach dem auf wissensbezogenen Ressourcen basierende Kernkompetenzen nur dann werthaltig sind, wenn sie einzigartig sind und nicht im Besitz eines Konkurrenten stehen, kann die Diffusion negative Auswirkung auf die wissensbasierten Wettbewerbsvorteile und somit die Wettbewerbsposition des Unternehmens haben (Liebeskind 1997, 645; Amelingmeyer 2002, 146; Matusik 2002b, 608; Mohr, Sengupta 2002, 282; Norman 2002, 178; Erickson, Rothberg 2005, 13). Dabei können die Folgen der Diffusion soweit gehen, dass die Existenz des Unternehmens bedroht ist (Freeman 2004, 1). Das Schadensausmaß einer unerwünschten Diffusion hängt davon ab, welche Inhalte betroffen sind und inwiefern diese außerhalb des Unternehmens nutzbar sind. Aus diesem Grund ist die Variabilität des Schadensausmaßes hoch (Claflin 2001, 2).

Wie in Abb. 23 dargestellt, geht die unerwünschte Diffusion von einer Reihe verschiedener interner und externer Akteure aus und kann einerseits auf primär personenbezogene und andererseits auf primär technologische Aktivitäten zurückgeführt werden. Externe Akteure stellen dabei Konkurrenten dar, die sich bestimmtes Wissen des Unternehmens aneignen wollen (Lux, Peske 2002, 38f). Zudem kann im Rahmen der Zusammenarbeit mit Kunden, Lieferanten[158], Kooperationspartnern oder Outsourcinganbietern Wissen von diesen Akteuren absorbiert werden. Darüber hinaus kann Wissen, das mit Kunden oder Lieferanten geteilt wurde, auch über Drittbeziehungen an direkte Konkurrenten diffundieren, die beispielsweise dieselben Kunden oder Lieferanten haben bzw. diese einsetzen (Mansfield 1985, 221; Bönte, Wiethaus 2005, 2). Im Speziellen trifft dies auch auf das Outsourcing von IT-Systemen oder Geschäftsprozessen zu, mit dem die Offenlegung von Wissen oder die Gewährung von Einblicken in sensitive Bereiche verbunden sein kann (Lei 1993, 37). Auch bei Kooperationen, die auf den Austausch von Wissen ausgerichtet sind, bestehen Diffusionspotentiale, da sich die Partner opportunistisch verhalten können, indem sie Freiräume zum Nachteil des Unternehmens nutzen (Badaracco 1991, 69; Fontanari 1996, 119; Hirschmann 1998, 38; de Laat 1999, 209; Oxley, Sampson 2004, 727).

[158] Im Falle von Kunden und Lieferanten kann das diffundierte Wissen zur Vor- oder Rückwärtsintegration eingesetzt werden (Porter 1989, 375ff).

Eine weitere Gruppe externer Akteure stellen Unternehmensberater, Zertifizierer, Finanzanalysten, externe Dienstleister[159] oder Mitarbeiter von Banken dar, die im Rahmen ihrer Tätigkeiten Wissen über ein Unternehmen erlangen, das für Konkurrenten werthaltig sein kann (McGonagle, Vella 1994, 53f; Knaese 2004, 71; Verfassungsschutz 2004b, 16; Meissinger 2006, 104). Auch Hacker können an einer Diffusion beteiligt sein und aus Eigenmotivation oder im Auftrag Dritter das Ziel verfolgen, sich Zugriff auf sensitive Inhalte zu verschaffen bzw. Sicherheitssysteme zu umgehen (Freeman 2004, 6). Weiterhin können Besucher externe Akteure einer unerwünschten Diffusion sein, da diese bei fehlender Beaufsichtigung und freiem Bewegungsraum Zugang zu sensitivem Wissen erlangen können (Meissinger 2006, 103).

Im Hinblick auf interne Akteure kann die Diffusion von Mitarbeitern[160] des Unternehmens ausgehen und durch deren bewusstes bzw. unbewusstes Zutun erfolgen. So können diese beispielsweise von Dritten ausgehorcht oder zur Verschaffung von Zugang bzw. Zugriff bewegt werden. Dabei ist den Mitarbeitern vielfach nicht bewusst, dass sie dem Unternehmen schaden. In diesem Fall sind die Mitarbeiter passiv in die Diffusion involviert. Mitarbeiter können aber auch durch Dritte fremdmotiviert werden und beispielsweise aufgrund von Bestechungen Wissen weitergeben. Darüber hinaus können Mitarbeiter auch aus Eigeninitiative als werthaltig empfundenes Wissen gezielt Konkurrenten anbieten. Die letzten beiden Fälle bezeichnen aktives Handeln seitens der Mitarbeiter (Maier 1992, 38ff; Liman 1999, 240; Freeman 2004, 1; Meissinger 2006, 97). Die in Abb. 23 abgetragenen Aktivitäten, an denen verschiedene Akteure beteiligt sind, können primär personenbezogen sein und beispielsweise Fehlverhalten, Einschleusung, Anwerbung, Aushorchung oder Abwerbung einschließen. Darüber hinaus können diese Aktivitäten auch primär auf den Einsatz von Technologien zurückgehen und beispielsweise Reverse Engineering, Angriffe auf IT-Systeme sowie das Abhören der Kommunikation und des Datenverkehrs umfassen. Neben einer von Akteuren zielgerichtet veranlassten Diffusion kann es auch der Fall sein, dass nicht autorisierte Personen in den Besitz sensitiven Wissens gelangen, ohne Maßnahmen ergriffen zu haben (McGonagle, Vella 1994, 51ff). So kann speziell im Kontext von IT-Systemen eine Wissensdiffusion durch das Versagen von Systemen verursacht werden (Peltier 2001, 13f). Somit kann die Diffusion allgemein betrachtet beabsichtigt und unbeabsichtigt erfolgen, allerdings auch zufällig oder aufgrund gezielter Absorbierung bzw. durch Penetration eines Dritten erfolgen (Kogut, Zander 1992, 384; de Laat 1999, 209; Teece 2000b, 134).

[159] Spezielle externe Dienstleister bieten Wissen, das sie z.B. über Unternehmen, Brachen oder Technologien gesammelt haben, zum Verkauf an. Sie sind dann gewissermaßen als Intermediäre tätig. Dabei können diese Anbieter auch im Auftrag von Konkurrenten, Kunden oder Lieferanten handeln (Lux, Peske 2002, 39f).

[160] Neben internen Mitarbeitern umfasst diese Gruppe auch Mitarbeiter von Fremdfirmen, Zeitarbeitnehmer, Praktikanten, Werkstudenten und Diplomanden. Aufgrund ihrer befristeten Tätigkeit und der vergleichsweise höheren Interfluktuation geht von dieser Gruppe ein erhöhtes Diffusionspotential aus, da beispielsweise unternehmensspezifisches Wissen zu bestimmten Themen oder unternehmensspezifischen Praktiken in anderen Unternehmen angewandt wird (Matusik, Hill 1998, 680ff; Verfassungsschutz 2004a, 9f).

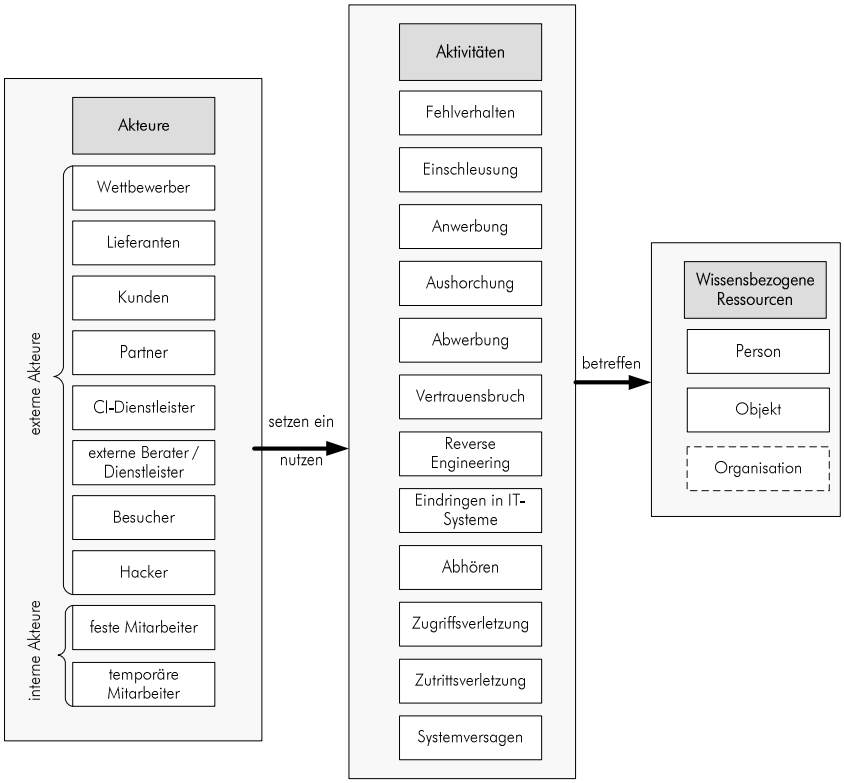


Abb. 23 Akteure und Aktivitäten im Kontext der Wissensdiffusion

Insgesamt verschwimmen die Grenzen zwischen Illegalität und Legalität zum Teil stark, weshalb eine große Grauzone besteht[161]. Das Ergreifen bestimmter Aktivitäten ist folglich auch von den ethischen Normen des jeweiligen Unternehmens bzw. der einzelnen Akteure abhängig. Im Hinblick auf die verschiedenen Typen von wissensbezogenen Ressourcen (siehe Abschnitt 2.2.3) kann sowohl in Objekten inkorporiertes Wissen, wie z.B. Produkte oder Konzepte, als auch personengebundenes Wissen wie Erfahrungen der Mitarbeiter betroffen sein. Organisatorisch verankertes Wissen, wie z.B. Wissen über Prozessabläufe, diffundiert vergleichsweise schwerer, da vielfach mehrere Wissensträger erforderlich sind, um das Wissen vollständig zu rekonstruieren.

5.4.2 Einzelrisiken

Personen: Wissensrisiken, der Ursachenkategorie Personen können auf das Verhalten bzw. auf Handlungen der Mitarbeiter zurückgeführt werden.

- **fahrlässiges Fehlverhalten (DP1)**: Fehlverhalten der Mitarbeiter kann sich sowohl auf den Umgang mit sensitiven Inhalten selbst als auch auf den Umgang mit IT-Systemen oder das Einhalten bestehender Sicherheitsrichtlinien beziehen. Darüber hinaus kann auch eine direkte Weitergabe sensitiver Inhalte erfolgen. So können sensitive Inhalte beispielsweise durch nicht autorisierte Personen zur Kenntnis genommen werden, wenn Mitarbeiter sorglos Inhalte übermitteln bzw. Funktionen zur verschlüsselten Kommunikation nicht nutzen (Fox 2003, 677; Freeman 2004, 6). Ferner kann sich eine Diffusion daraus ergeben, dass Mitarbeiter unzureichend mit Passwörtern umgehen[162] (Bitkom 2003, 22f; Eckert 2003, 15; Rossa 2004, 70; BSI 2006, 531). In diesem Kontext

[161] Nach Liman (1999, 46) variieren Gesetzessituationen im internationalen Kontext stark, wodurch die Abgrenzung zwischen Legalität und Illegalität erschwert wird.

[162] Ein ungeeigneter Umgang schließt beispielsweise Weitergabe, Aufbewahrung an nicht sicheren Orten, Nichterfüllung von Anforderungen an deren Komplexität, Verwendung von Einheitspasswörtern oder mangelnde Aktualisierung ein.

kann eine unerwünschte Diffusion von Wissen auch darauf zurückgehen, dass Mitarbeiter beim Verlassen des Arbeitsplatzes auf eine Passwortsicherung des Arbeitsplatzrechners verzichten und somit eine fehlende Benutzertrennung vorliegt, da andere Mitarbeiter oder Dritte unautorisiert auf sensitive Inhalte zugreifen können (Bitkom 2003, 26; Kruth 2004, 200). Weiterhin kann ein sorgloser Umgang mit sensitiven Inhalten selbst oder den entsprechenden Endgeräten (z.B. Notebooks auf Geschäftsreisen) die Diffusion von Wissen ermöglichen (BSI 2006, 532). Zudem kann vertrauensseliges Verhalten gegenüber Dritten, eine Aushorchung bzw. das Social Engineering erleichtern (Hirschmann, Romeike 2004, 13; Humpert 2004, 17; Meissinger 2006, 89). Neben einem Fehlverhalten im Umgang mit Kommunikationstechnologien, Passwörtern oder Hardware, das Dritten sensitive Inhalte zugänglich bzw. zugreifbar macht, können Wissensrisiken auch auf die aktive Weitergabe sensitiver Inhalte zurückgehen. So können beispielsweise E-Mails oder Faxe an unautorisierte Empfänger versandt werden, sensitive Inhalte in elektronischen Ablagestrukturen in Ordnern mit einer niedrigeren Berechtigungsstufe abgelegt oder physische Dokumente offen zugänglich gemacht werden. Zudem kann aufgrund einer fehlerhaften Einschätzung des Wertes bzw. der Vertraulichkeit von Inhalten eine Verteilung an nicht autorisierte Personen erfolgen (McGonagle, Vella 1994, 49; Freeman 2004, 6). Schließlich kann fahrlässiges Fehlverhalten auch auf mangelnde Kompetenzen zurückgeführt werden[163].

- **vorsätzliches Fehlverhalten (DP2)**: Neben einer durch Fahrlässigkeit verursachten Diffusion kann diese auch auf Vorsatz zurückgehen. Dabei können Mitarbeiter organisatorische Richtlinien oder ethische Normen missachten, um dem Unternehmen aus Eigeninteresse oder zu Gunsten eines Dritten zu schaden. Mitarbeiter können beispielsweise Zugriffsrechte missbrauchen, Sicherheitsvorkehrungen umgehen, gezielt Passwörter an Dritte weitergeben bzw. diese anbieten[164] oder vorsätzlich sensitive Inhalte weitergeben (Kruth 2004, 129f; BSI 2006, 689, 735). Aktives Handeln der Mitarbeiter und somit mangelnde Loyalität dem Unternehmen gegenüber hat bestimmte Ursprünge bzw. Motivationsfaktoren. Monetäre Anreize stellen ein klassisches Motiv dar, das in einer Vielzahl der Fälle ausschlaggebend ist. Zudem können die Verärgerung über den Arbeitgeber, Unzufriedenheit (z.B. ungerechte Behandlung) oder ideologische Diskrepanzen eine weitere Motivation darstellen, die zum Eigenangebot führt bzw. für Fremdmotivation empfänglich macht (Lux, Peske 2002, 87; Freeman 2004, 1). Im Hinblick auf einen anstehenden Unternehmenswechsel kann auch die Veränderung des Vertrauensstatus zum Arbeitgeber ausschlaggebend sein (Freeman 2004, 6).

[163] Für Informationskompetenz siehe (Kern et al. 1998, 14; Abell, Oxbow 2002, 128ff).

[164] Derartigen eigenmotivierten Angeboten stehen Unternehmen allerdings vielfach skeptisch gegenüber, da es sich um eine Irreführung handeln könnte und zudem potentielle Reputationsverluste bei Öffentlichwerden der Inanspruchnahme eine Folge wären (Maier 1992, 39).

Prozesse: Eine unerwünschte Diffusion der Kategorie Prozesse kann mit Schwächen von Prozessen, organisatorischen Richtlinien oder Maßnahmen, die seitens des Unternehmens ergriffen wurden, in Zusammenhang stehen.

- **Zutrittsverletzung (DO1)**: Ein Risiko in Bezug auf eine unerwünschte Diffusion kann sich daraus ergeben, dass Personen unautorisiert Zutritt erhalten und so Kenntnis von sensitiven Inhalten nehmen können. Dies kann darauf zurückzuführen sein, dass Zutrittskontrollen fehlen, unzureichend definiert oder umgesetzt werden, da so unautorisierte Personen (z.B. Mitarbeiter, externe Partner, Besucher) Zugang zu sensitiven Inhalten erhalten können (Liebeskind 1997, 633f; Meissinger 2006, 103). So kann beispielsweise eine geringe Einschränkung eines Besuchers oder Partners zur Folge haben, dass Dokumente von Schreibtischen oder Inhalte nicht passwortgeschützter Rechner zur Kenntnis genommen werden und so Wissen diffundiert.
- **Zugriffsverletzung (DO2)**: Ein Wissensrisiko in Bezug auf die Diffusion ist darin zu sehen, dass interne und externe Personen unautorisiert Zugriff auf Inhalte erhalten und so Kenntnis nehmen können. Risiken in Bezug auf das Management von Zugriffsrechten können verschiedene Ursprünge haben und die Vergabe, Dynamisierung sowie die Einhaltung der Zugriffsrechte durch entsprechende Kontrollen betreffen. Die Vergabe der Rechte basiert dabei auf der Zugriffskontrollstrategie und eines daraus abgeleiteten Berechtigungskonzeptes, während dessen technische Umsetzung durch ein Zugriffskontrollsystem erfolgt (Stiemerling et al. 2000, 319). Dabei können die Zugriffsrechte zu umfassend definiert sein. In diesem Fall, ist der Zugriff streng genommen autorisiert, allerdings nimmt bedingt durch die freigebige Vergabe die Wahrscheinlichkeit zu, dass aus der Sicht der Unternehmung unerwünschte Zugriffe erfolgen. Neben der einmaligen Definition von Zugriffsrechten ist auch deren laufende Anpassung erforderlich, da sich die Aufgaben von Mitarbeitern im Unternehmen verändern oder diese aus dem Unternehmen ausscheiden. Analoges gilt für externe Partner, wenn beispielsweise Geschäftsbeziehungen beendet werden (Rogulla, Walther 2003a, 21; Herwig, Schlabitz 2004, 290). Derartige Veränderungen erfordern die umgehende Anpassung bzw. Dynamisierung der Zugriffsrechte, da sich der Status der Autorisierung mit diesen Ereignissen verändert. Unterbleibt dies steigt der Erwartungswert des Risikos einer unerwünschten Diffusion, da im Falle des Ausscheidens aus dem Unternehmen oder der Beendigung einer Geschäftsbeziehung mit einem Partner die Grundlage zur Autorisierung fehlt und von nun an Zugriffe dieser Nutzer unautorisiert erfolgen. Neben einer potentiellen Risikobehaftung des Zugriffskontrollkonzeptes, kann auch das -system mit Risiken einhergehen, wenn es technische Schwachstellen enthält, die ein Umgehen des Systems leicht möglich machen. Insbesondere bei einer unternehmensexternen Zugreifbarkeit wird das Risikopotential erhöht. So kann beispielsweise eine fehlende Einschränkung der möglichen Anzahl von Anmeldeversuchen (z.B. über Brute-Force Attacken) die Entschlüsselung vereinfachen. Weiterhin kann die Übertragung der Benutzer-

informationen im Klartext oder bei zu geringer Verschlüsselung ebenso eine Aushebelung der Zugriffskontrolle und somit eine unerwünschte Diffusion wahrscheinlicher machen (Manthei, Schmidt 2005, 78; BSI 2006, 544, 626). Zusätzlich erhöht sich das Risikopotential in Bezug auf das Management der Zugriffsrechte, wenn externe Partner einbezogen werden (Keitsch 2000, 32).

- **unkontrollierter Einsatz temporär beschäftigter Mitarbeiter (DO3)**: Das Risiko einer Diffusion von Wissen geht zudem vom Einsatz kurzfristig beschäftigter Mitarbeiter (z.B. Zeitarbeitnehmer) aus, da diese Mitarbeiter innerhalb kurzer Zeit die Arbeitgeber wechseln. Auf diese Weise kann unternehmensspezifisches Wissen im Allgemeinen und Wissen über Verfahrensweisen oder Prozesse im Speziellen diffundieren. Ebenso erhalten Praktikanten, Werkstudenten und Diplomanden Einblicke in das Unternehmen bzw. eignen sich Wissen an, das im Zuge der Fluktuation zu anderen Unternehmen diffundieren kann (Matusik, Hill 1998, 680ff; Verfassungsschutz 2004a, 9f). Dieses Risiko wird allerdings dadurch begrenzt, dass die Internalisierung von Wissen über Abläufe zum Teil einen hohen zeitlichen Aufwand und eine entsprechende Einbindung voraussetzt und dies im Falle kurzfristig beschäftigter Mitarbeiter vielfach nicht der Fall ist.
- **unkontrollierte interorganisatorische Zusammenarbeit (DO4)**: Ein Wissensrisiko in Bezug auf die unerwünschte Diffusion geht auch von einer unkontrollierten Zusammenarbeit mit anderen Unternehmen und dabei insbesondere Kooperationspartnern aus. Gerade im Hinblick auf einen effizienten Wissenstransfer wird die Zusammenarbeit durch den Einbezug vieler Mitarbeiter intensiviert[165]. Jedoch steigt bedingt durch die Intensität der Zusammenarbeit die Wahrscheinlichkeit, dass Partner Kenntnis von Wissen erhalten, das ihnen aus Gründen der Vertraulichkeit nicht zugänglich sein sollte, da die Kontrollierbarkeit bei zunehmender Zahl an Interaktionspunkten abnimmt (Hamel et al. 1989, 136; Lei 1993, 40; Oxley, Sampson 2004, 727)[166]. Das Risiko der fehlenden Kontrollierbarkeit wird zusätzlich dadurch verstärkt, wenn nicht geregelt ist, welches Wissen Gegenstand der Kooperation ist, wie der Austausch erfolgt und inwiefern das Wissen außerhalb der Kooperationsbeziehung (z.B. in anderen Produkten oder Märkten) genutzt werden kann (Lei 1993, 36; Kronen 1994, 69; Fleischer 1997, 237f; Hirschmann 1998, 31; de Laat 1999, 209; Desouza, Vanapalli 2005, 80f). Auch im Bereich des Outsourcing sind Regelungen für die Zusammenarbeit und die Einhaltung von Sicherheitsanforderungen erforderlich.
- **unkontrollierte Veröffentlichung (DO5)**: Risiken in Bezug auf eine unerwünschte Diffusion von Wissen können auch durch ein unzureichendes Vorgehen bei Veröffentlichung hervorgerufen werden. Dies betrifft beispielsweise externe Publikationen (z.B. Fachzeitschriften, Tageszeitun-

[165] Dazu werden z.B. gemeinsame Projektteams gebildet, gemeinsame Produktionsstandorte genutzt oder Mitarbeiter über die beteiligten Partnerunternehmen rotiert. Siehe hierzu auch Infrastruktur in Abschnitt 5.4.1.

[166] Bei einer intensiven unternehmensübergreifenden Zusammenarbeit wie z.B. in Kooperationen kann beispielsweise aufgrund des verbesserten Zugangs das Wissen aus Prototypen destilliert werden (Kogut, Zander 1992, 393; Appleyard, Kalsow 1999, 288; Nieto, Pérez-Cano 2004, 120ff; Erickson, Rothberg 2005, 11).

gen, News auf Websites), interne Publikationen (z.B. Mitarbeiterzeitung) oder externe Berichterstattung zu immateriellen Vermögenswerten (siehe Abschnitt 2.3.4). Eine zu freigebige Veröffentlichung sensitiver Inhalte sowie die fehlende Beachtung der Summe aller Veröffentlichungen und ihres Zusammenhangs, kann zur Folge haben, dass Konkurrenten im Rahmen legaler Konkurrentenanalyse und -beobachtung durch einzelne oder die Kombination mehrerer Veröffentlichungen zum Nachteil des Unternehmens in den Besitz sensitiver Inhalte gelangen bzw. diese erfolgreich rekonstruieren. So kann beispielsweise das Wissen über ein Produkt durch Informationen auf der Website, Interviews in Tageszeitungen, interne Mitarbeiterzeitungen, die weitergegeben wurden, oder Fachartikeln von Entwicklungsingenieuren durch Konkurrenten kombiniert und somit rekonstruiert werden (McGonagle, Vella 1994, 294ff).

Systeme: Die unerwünschte Diffusion sensitiver Inhalte kann auch auf Schwächen bzw. Versagen der IT des Unternehmens zurückgeführt werden und ist Gegenstand der nachfolgenden Betrachtungen.

- **mangelnde Sicherung der IT-Systeme (DS1)**: Eine Vielzahl an Mängeln bzw. Schwachstellen im Bereich der IT-Sicherheit können eine Ursache für das Risiko einer unerwünschten Diffusion von Wissen darstellen. Aufgrund des Umfangs der verschiedenen Schwachstellen im Bereich der IT-Sicherheit wird an dieser Stelle auf einschlägige Werke, wie z.B. (BSI 2006; Eckert 2006), verwiesen und nur exemplarisch auf einige Schwachstellen eingegangen. So kann sich das Risiko einer unerwünschten Diffusion daraus ergeben, dass Firewalls[167] nicht eingesetzt werden oder bei deren Einsatz die Konfiguration der Regeln zu wenig restriktiv ist (BSI 2006, 190ff)[168]. Weiterhin kann der fehldende Einsatz von Virenscanneren zur Folge haben, dass Systeme durch Schädlingsprogramme infiziert werden und sich dies wiederum auf die Exklusivität der Wissenselemente auswirkt. Ebenso kann das fehlende Identifizieren und Schließen von Schwachstellen in Betriebs- und den Anwendungssystemen zur Folge haben, dass Schadsoftware die IT-Systeme befällt (BSI 2006, 4, 1629).

  Neben dem unternehmensinternen Einsatz und den daraus erwachsenden Sicherheitsanforderungen erfolgt vielfach im Rahmen von Partnerschaften eine unternehmensübergreifende gemeinsame Nutzung von IT-Systemen oder spezifischen Anwendungen. Neben der interorganisatorischen Nutzung zwischen Partnern erfolgt eine externe Öffnung der IT-Systeme auch für Mitarbeiter im Außendienst oder im Rahmen der Telearbeit, damit Mitarbeiter auf die für die Tätigkeiten erforderlichen Inhalte zugreifen können. Auch dies verbreitert die potentiellen Angriffsmöglichkeiten und erhöht somit das Risikopotential. Risiken sind in diesem Zusammenhang darin zu sehen, dass bei einem unternehmensübergreifenden Austausch von Daten öffentliche Netze genutzt werden

[167] Für weitere Details zu Firewalls und deren Konfiguration siehe (Strobel 2003, 95ff).

[168] Als weiteres Beispiel für ein Risiko kann die Verwendung aktiver Inhalte in Websites oder E-Mails sowie Web-to-Host Konzepte zur Interaktion mit externen Partnern angeführt werden, da deren automatisch ausgeführter Code Schadfunktionen enthalten kann (Hawthorn 2002, 46; Kruth 2004, 135; BSI 2006, 523).

und sich dadurch Angriffsmöglichkeiten in Bezug auf eine unerwünschte Diffusion ergeben (BSI 2006, 431f)[169]. Zudem ergibt sich aus der gemeinsamen Nutzung der Systeme das Risiko, dass unautorisierte Durchgriffe durch den Partner erfolgen (Keitsch 2000, 32; Krcmar, Junginger 2003, 253).

- **technisches Versagen / Fehlfunktionen (DS2)**: Wissensrisiken im Bereich der Diffusion können auch dadurch hervorgerufen werden, dass IT-Systeme, einzelne Komponenten dieser oder sonstige technische Systeme versagen. Zudem können auch Softwarefehler eine unerwünschte Diffusion zur Folge haben (BSI 2006, 592, 611f). So kann beispielsweise das Versagen von Sicherheitssystemen einen ungehinderten Zugriff auf sensitive Inhalte ermöglichen oder das Ausfallen von Zugangskontrollen unautorisierten Personen Zugang zur Folge haben. Im Bereich der Kommunikation bzw. des Datenverkehrs können ebenfalls Fehlfunktionen dazu führen, dass sensitive Inhalte an unautorisierte Dritte diffundieren.

externe Faktoren: Neben internen Ursachen der Kategorien Personen, Prozesse und Systeme kann die unerwünschte Diffusion auch auf externe Faktoren, die außerhalb des Verantwortungsbereiches des Unternehmens liegen, zurückgeführt werden, denen die nachfolgend erörterten Risiken zugeordnet werden können.

- **Aushorchung (DE1)**: Das Risiko einer unerwünschten Diffusion von Wissen kann dadurch hervorgerufen werden, dass Dritte versuchen z.B. unter Vorspiegelung falscher Identitäten Mitarbeiter auszuhorchen. So können sich Dritte beispielsweise als Kunden oder Mitarbeiter einer Forschungseinrichtung, die Befragungen durchführt, ausgeben und die entsprechenden internen Mitarbeiter z.B. telefonisch kontaktieren, um so an Wissen zu gelangen (Maier 1992, 42; McGonagle, Vella 1994, 53f; Liman 1999, 240). Im Hinblick auf das Ausspionieren von Zugriffsdaten kommt der Aushorchung, die in diesem Fall auch als Social Engineering oder Social Hacking bezeichnet wird, ebenfalls eine entscheidende Bedeutung zu. So können sich Dritte am Telefon beispielsweise als Mitarbeiter der IT-Abteilung oder eines IT-Dienstleisters ausgeben, um an die Zugangsdaten zu gelangen (Hirschmann, Romeike 2004, 13; Humpert 2004, 17).
- **Einschleusung (DE2)**: Eine unerwünschte Diffusion von Wissen kann darauf zurückgeführt werden, dass Dritte unter Vorspiegelung falscher Tatsachen bzw. falscher Identitäten externe Personen als Mitarbeiter in das Unternehmen einschleusen, die in ihrem Namen handeln. Diese Mitarbeiter können sich Zutritt und Zugriff zu sensitiven physisch oder elektronisch dokumentierten Inhalten verschaffen, interne Mitarbeiter aushorchen oder z.B. im Rahmen von Meetings oder der internen Unternehmenskommunikation in Erfahrung gebrachtes Wissen an die Auftraggeber transferieren. Neben der Einschleusung von Mitarbeitern können auch von Dritten angeworbene Test-

[169] Das Risiko besteht primär in der Verwendung unsicherer Protokolle. Die Protokolle FTP (File Transfer Protocol), http (Hypertext Transfer Protocol), Telnet oder POP3 (Post Office Protocol) übertragen in Klartext.

kunden z.B. bei Produktpräsentationen eingeschleust werden (Erickson, Rothberg 2005, 13). Durch eine Einschleusung kann es über einen längeren Zeitraum zu einer Diffusion von Wissen kommen (Maier 1992, 37f; Liman 1999, 240).

- **Anwerbung (DE3)**: Ebenso wie die Einschleusung von Mitarbeitern ist auch die Anwerbung von Mitarbeitern extern getrieben. Der Unterschied besteht jedoch darin, dass in diesem Fall interne Mitarbeiter des Unternehmens durch Dritte überzeugt werden, in deren Namen zu handeln und sensitive Inhalte weiterzugeben. Somit handeln die Mitarbeiter zwar bewusst, allerdings betrifft die primäre Ursachenzuordnung Dritte, von denen die Anwerbung ausgeht. Neben einer Überzeugung mittels verschiedener monetärer und nicht-monetärer Anreize kann eine Anwerbung auf eine Erpressung des entsprechenden Mitarbeiters zurückgehen. Ebenso wie bei Einschleusung kann im Falle der Anwerbung die Diffusion von Wissen über einen längeren Zeitraum erfolgen. In beiden Fällen ist die Entdeckungswahrscheinlichkeit relativ gering und somit ein hohes Risikopotential gegeben (Maier 1992, 38ff; Liman 1999, 240).
- **opportunistisches Verhalten der Partner (DE4)**: Mit Kooperationen geht allgemein das Risiko des opportunistischen Verhaltens des Partners einher (Das 2005, 707). Williamson bezeichnet opportunistisches Verhalten als das Verfolgen eigener Interessen unter Einsatz von Arglist (Williamson 1975, 6). Arglist kann sich beispielsweise auf Lügen, Betrug, Diebstahl, Verzerrung oder Verschleierung beziehen (Williamson 1985, 47). Opportunistisches Verhalten setzt ein Motiv, den Zugang zu privilegierten Informationen und die Möglichkeit unentdeckt handeln zu können, voraus (Davies 2000, 45ff). Es kann angenommen werden, dass opportunistisches Verhalten jeder Kooperation inhärent ist, allerdings dieses Potential unterschiedlich genutzt wird, da beispielsweise negative Konsequenzen in Bezug auf die Reputation in der Branche befürchtet werden. Dieses Verhalten in Kombination mit einem durch die Kooperation bedingten privilegierten Zugang kann verschiedene andere Risiken, wie z.B. die Anwerbung, Abwerbung oder Diebstahl sensitiver Inhalte, bedingen.

  Neben Partnern kann eine unerwünschte Diffusion auch vom Einsatz externer Dienstleister, wie z.B. Berater, Zertifizierer oder Wirtschaftsprüfer, ausgehen, wenn diese Wissen, das ihnen im Rahmen ihrer Tätigkeiten zugänglich gemacht wurde, in anderen Unternehmen anwenden. Eine derartige Weitergabe kann dabei gegen die ethischen und vertraglichen Grundsätze des Berufsstandes verstoßen und geht mit einem Vertrauensbruch dem Auftraggeber gegenüber einher (McGonagle, Vella 1994, 53f; Knaese 2004, 71; Verfassungsschutz 2004b, 16; Meissinger 2006, 104). Zudem erhält auch Reinigungspersonal vielfach außerhalb der Bürozeiten Zugang zu Büroräumen. Diese Dienstleister können das entgegengebrachte Vertrauen brechen, wenn sie beispielsweise aus Eigeninitiative handeln oder sich aufgrund einer Anwerbung durch Dritte Zutritt und Zugriff zu sensitiven Inhalten verschaffen und diese weitergeben (BSI 2006, 489).

- **unzureichende Vertraulichkeitswahrung durch Partner (DE5)**: In Kooperationen oder Geschäftsbeziehungen kann das Risiko auftreten, dass sensitive Inhalte potentiell über mehrere Stationen an unautorisierte Dritte, denen diese Inhalte zum Vorteil gereichen, diffundiert. Eine derartige Diffusion kann beispielsweise darauf zurückgeführt werden, dass Lieferanten auch gleichzeitig für Konkurrenten tätig sind oder Konkurrenten über die gleichen Kunden verfügen, mit denen Wissen z.B. im Rahmen von Produktentwicklungen oder -verbesserungen ausgetauscht wird. Diese Risiken stehen in Zusammenhang mit einer unzureichenden Vertraulichkeitswahrung der Partner bzw. Dienstleister, die allerdings nicht auf opportunistisches Verhalten (siehe **DE4**) zurückgehen, sondern vielmehr auf Fahrlässigkeit. Diese Risiken sind schwer erfassbar, da vielfach komplexe und mehrstufige Beziehungsgeflechte an Drittbeziehungen bestehen, über die Wissen an nicht autorisierte Dritte im Allgemeinen und Konkurrenten im Speziellen diffundieren kann (Fontanari 1996, 195; Bönte, Wiethaus 2005, 2; Erickson, Rothberg 2005, 11).
- **Reverse Engineering (DE6)**: Das Risiko einer unerwünschten Diffusion kann sich auch daraus ergeben, dass Produkte des Unternehmens durch Dritte gezielt untersucht bzw. in ihre einzelnen Komponenten zerlegt werden und das zugrunde liegende Wissen erfolgreich rekonstruiert wird. Es wird dabei aus einem bestehenden Produkt ein Plan zu dessen Herstellung oder Erkenntnisse zur Funktionsweise bzw. zu den Zusammenhängen der Einzelkomponenten destilliert. Dabei werden nahezu identische Abbildungen des ursprünglichen Produktes erstellt, die selbst von Experten vielfach nur schwer von den Originalen zu unterscheiden sind. Besonders evident ist das Risikopotential derartiger Maßnahmen, wenn man die Häufung der Fälle von Produktpiraterie betrachtet[170]. Der Erwartungswert einer erfolgreichen Reverse Engineering Maßnahme durch Dritte wird beispielsweise davon beeinflusst, wie komplex und unternehmensspezifisch das zugrunde liegende Wissen ist und ist somit von den in Abschnitt 2.2.4 dargestellten Eigenschaften von Wissen abhängig (Kogut, Zander 1992, 393; Appleyard, Kalsow 1999, 288; Nieto, Pérez-Cano 2004, 120ff; Erickson, Rothberg 2005, 11). Diese Problematik ist dann besonders ausgeprägt, wenn Produkte in Länder exportiert werden, in denen gewerbliche Schutzrechte wie Patente oder Copyrights nicht durchsetzbar sind (Maskus 2003, 192).
- **Diebstahl (DE7)**: Der Diebstahl von physisch oder elektronisch dokumentiertem Wissen, der in Abhängigkeit der redundanten Vorhaltung, Wiederherstellbarkeit und Rekonstruierbarkeit des Wissens zu einem mehr oder minder hohen Wissensverlust (siehe VE3) führen kann (siehe 5.3.2), stellt zugleich primär eine Quelle für die unerwünschte Diffusion von sensitiven Inhalten dar. So können z.B. durch den Diebstahl von physischen Dokumenten oder Hardware sensitive Inhalte an

[170] Weltweit beträgt der volkswirtschaftliche Schaden durch Produktpiraterie nach Schätzungen der EU oder der internationalen Handelskammer 300 bis 660 Mrd. €. Somit wären etwa 5-9% Prozent des Welthandels Fälschungen. Für deutsche Unternehmen dürfte der Schaden jährlich etwa bei 20 bis 30 Mrd. € liegen. (Wildemann 2007, 37). Siehe hierzu auch http://www.iccccs.org/cib 1.8.2006 /.

nicht autorisierte Dritte diffundieren und somit durch die Einschränkung der Exklusivität deren Wert abnehmen (Liman 1999, 238f; Desouza, Awazu 2004, 6; Freeman 2004, 6).

- **Abhören (DE8)**: Eine unerwünschte Diffusion kann ferner dadurch verursacht werden, dass Telekommunikationsnetze oder der elektronische Datenverkehr unter Einsatz verschiedenster Technologien, wie z.B. Drahtfunk, Richtmikrofone, Telefonwanzen oder manipulierte Handys, abgehört werden. Die Übertragung kann über Kabelverbindungen, wie z.B. Glasfaser-, Kupferkabel oder Funkverbindungen erfolgen, wobei nahezu keine vollkommen abhörsichere Übertragung möglich ist, was zur Folge hat, dass das Risiko des Abhörens der Kommunikation bzw. des Datenverkehrs nicht vermieden werden kann. Der erforderliche Aufwand zum Abhören bestimmter Leitungen unterscheidet sich allerdings. In Bezug auf die Telekommunikation kann das Abhören durch direktes Anzapfen des Telefonkabels oder der vermittelnden Telekommunikationsanlage erfolgen. Erfolgt die Telefonie des Unternehmens über Internetprotokolle (VoIP), ist das Abhören von Telefongesprächen sehr risikobehaftet, da alle Sprachinformationen innerhalb eines IP-Medienstroms übertragen werden. Analog dazu können auch Räume in Unternehmen, Mobiltelefone etc. durch Dritte abgehört werden, um so an sensitive Inhalte zu gelangen (Lux, Peske 2002, 83ff; Bitkom 2003, 30f; Verfassungsschutz 2004b, 16; BSI 2006, 677, 682, 689, 714; Meissinger 2006, 68ff; Niedermeier, Huth 2006, 3ff).
- **Angriff auf IT-Systeme (DE9)**: Darüber hinaus kann das Risiko einer unerwünschten Diffusion von Wissen auch dadurch hervorgerufen werden, dass externe Angriffe auf die IT-Systeme des Unternehmens erfolgen. Dabei können von Dritten Lücken in Sicherheitssystemen identifiziert und genutzt werden. So können beispielsweise Port Scanner eingesetzt werden, um nicht durch die Firewall geschützte Ports zu identifizieren und so in IT-Systeme einzudringen mit der Konsequenz des Zugriffs auf sensitive Inhalte (Kruth 2004, 165). Im Speziellen kann Schadsoftware (z.B. Viren, Würmer, Spyware und Trojanische Pferde) eingeschleust werden, wobei in diesem Kontext Trojanische Pferde oder Spyware von Relevanz sind, da diese zum Ausspionieren von Passwörtern eingesetzt werden und so einen unautorisierten Zugriff ermöglichen können (BSI 2006, 691f, 693ff, 808f). Brute-Force Attacken können zur Folge haben, dass mittels einer algorithmischen Generierung von Passwortkombinationen die tatsächlichen Passwörter entschlüsselt werden und so ein unautorisierter Zugriff erfolgen kann (Verfassungsschutz 2004b, 16; Maier et al. 2005, 129f; Manthei, Schmidt 2005, 77ff; Eckert 2006, 341f). Ferner können Angriffe darauf fokussiert sein, Übertragungswege umzuleiten (z.B. durch die Manipulation von Routingtabellen), um so an sensitive Inhalte zu gelangen (BSI 2006, 724, 726). Die Angriffe gehen dabei oftmals von Hackern aus, die Schadsoftware in Umlauf bringen. Deren Aktivitäten sind vielfach nicht wirtschaftlich motiviert. Es kann aber auch der Fall sein, dass Angriffe von direkten Konkurrenten durchgeführt bzw. veranlasst werden, um im Rahmen der Betriebsspionage beispielsweise sensiti-

ve Inhalte oder Passwörter zu beschaffen. Ferner können auch Hacker sensitive Inhalte, in deren Besitz sie im Zuge der Angriffe gelangt sind, Unternehmen anbieten. Ungeachtet dessen wie die Angriffe motiviert wurden, geht eine Diffusion von sensitiven Inhalten potentiell mit der Entwertung der sensitiven Inhalte einher, wobei das Schadensausmaß des Risikos dann zunimmt, wenn diffundierte Inhalte in den Besitz direkter Konkurrenten gelangen.

- **Sicherheitsverstoß durch Partnern (DE10)**: Neben dem unternehmensinternen Betrieb der IT-Systeme und Anwendungen kann dieser auch an Dritte im Rahmen von Outsourcingabkommen vergeben sein und somit außerhalb des direkten Einflussbereiches und der Verantwortung des Unternehmens liegen. Ein Risiko besteht in diesem Kontext darin, dass definierte Sicherheitsanforderungen von Dritten aufgrund mangelnder Sorgfaltspflichten nicht erfüllt werden. Das Risikopotential ist dabei vielfach zu Beginn des Outsourcingabkommens höher (BSI 2006, 434ff, 439). Bezüglich Outsourcing verzichtet nach einer Studie von Ernst & Young (2004, 3) ein Großteil der untersuchten Unternehmen auf die regelmäßige Überprüfung des Outsourcingpartners im Hinblick auf die Einhaltung der Anforderungen in Bezug auf die IT-Sicherheit.
- **Anwendung von Wissen durch ehemalige Mitarbeiter (DE11)**: Bedingt durch die Interfluktuation von Mitarbeitern kann Wissen diffundieren, da ehemalige Mitarbeiter unternehmensspezifisches Wissen (z.B. über Prozesse oder Verfahrensweisen) in anderen Unternehmen anwenden können. Dadurch wird die Exklusivität dieses Wissens negativ beeinträchtigt (Matusik, Hill 1998, 687). Neben der Anwendung von unternehmensspezifischem Wissen kann es auch der Fall sein, dass Mitarbeiter dokumentiertes Wissen zu einem neuen Arbeitgeber transferieren[171].

[171] Dabei ist zu beachten, dass in diesem Fall neben den im Unternehmen erworbenen Kompetenzen auch dokumentiertes Wissen wie Konzepte, Verfahrensanweisungen oder Prozessbeschreibungen in das neue Unternehmen transferiert werden können und auf diese Weise eine unerwünschte Diffusion von Wissen erfolgen kann. Als Beispiel kann in diesem Kontext die López-Affäre herangezogen werden. 1993 wechselte der spanische Top-Manager López von General Motors mit sieben weiteren Führungskräften zu Volkswagen. Dabei wurden im Zuge der Abwanderung nachweislich sensitive Dokumente wie z.B. Pläne zur Entwicklung eines neuen Fahrzeugmodells zu Volkswagen in großem Umfang transferiert. Dies zog einen langwierigen Prozess mit der Anklage des Verrats von Betriebsgeheimnissen ebenso wie hohe Schadensersatzforderungen nach sich (Liebeskind 1997, 635). Dabei ist allerdings immer fraglich, inwiefern monetärer Schadensersatz die Diffusion von sensitivem Wissen und den damit verbundenen Verlust an Exklusivität adäquat kompensieren kann. Selbst wenn derartigen Aktivitäten hohe Strafen gegenüberstehen, so können die Anreize für diese Aktivitäten sehr hoch sein bzw. von den jeweils begünstigten Dritten entsprechend hoch vergütet werden. General Motors machte Schadensersatzansprüche in Höhe von 100 Mio. $ geltend.

5.4.3 Diskussion

Bei einer zusammenfassenden Betrachtung der Risiken der Wissensdiffusion ist festzuhalten, dass eine Vielzahl interner und externer Akteure aktiv oder passiv an der Diffusion beteiligt sein können. Dies hat zur Folge, dass Risiken der Wissensdiffusion einen hohen Variantenreichtum aufweisen. Analog zu den Wissensrisiken im Zusammenhang mit Wissensverlusten sind auch Risiken im Kontext dieses Konzeptes den vier Kategorien Personen, Prozesse, Systeme und externe Faktoren zuordenbar. Aufgrund der Vielzahl externer Akteure und der Außenorientierung des Konzeptes sind Wissensrisiken der letztgenannten Kategorie von besonderer Relevanz. Wissensdiffusionen, die der Kategorie Personen zugeordnet werden, stehen in einem primären Zusammenhang mit Fehlverhalten der Mitarbeiter. Im Hinblick auf Prozesse gehen Wissensdiffusionen auf eine unzureichende Definition der Prozesse in den Bereichen Zugang und Zugriff, Einsatz temporärer Mitarbeiter sowie Zusammenarbeit mit Partnern zurück. Ebenso sind aufgrund der Außenwirkung dieser Risikokategorien Schwächen bei Prozessen zur Veröffentlichung eine mögliche Diffusionsquelle. In Bezug auf Systeme gehen von der unzureichenden Sicherung der IT-Systeme ebenso wie von technischem Versagen bzw. Fehlfunktionen mögliche Diffusionen aus. Wissensdiffusionen im Zusammenhang mit externen Faktoren zielen auf personelle Schwachstellen ab, indem Mitarbeiter ausgehorcht, abgeworben oder eingeschleust werden. Mit einer erfolgreichen Abwerbung kann dann die Diffusion weiteren Wissens durch entsprechende Anwendung der abgewanderten Mitarbeiter einhergehen.

Kategorie	No	Wissensrisiko
Personen	DP1	fahrlässiges Fehlverhalten
	DP2	vorsätzliches Fehlverhalten
Prozesse	DO1	Zutrittsverletzung
	DO2	Zugriffsverletzung
	DO3	unkontrollierter Einsatz temporärer Mitarbeiter
	DO4	unkontrollierte interorganisatorische Zusammenarbeit
	DO5	unkontrollierte Veröffentlichung
Systeme	DS1	mangelnde Sicherung der IT-Systeme
	DS2	technisches Versagen / Fehlfunktionen
externe Faktoren	DE1	Aushorchung
	DE2	Einschleusung
	DE3	Anwerbung
	DE4	opportunistisches Verhalten der Partner
	DE5	unzureichende Vertraulichkeits-wahrung durch Partner
	DE6	Reverse Engineering
	DE7	Diebstahl
	DE8	Abhören
	DE9	Angriff auf IT-Systeme
	DE10	Sicherheitsverstoß durch Partner
	DE11	Anwendung von Wissen durch ehemalige Mitarbeiter

Tab. 9 Wissensrisiken der Kategorie Wissensdiffusion

Weiterhin gehen Risiken der Wissensdiffusion von unzureichendem Verhalten der Partner aus, indem sich diese entweder opportunistisch verhalten, die Vertraulichkeit nicht wahren oder gegen Sicherheitsrichtlinien verstoßen. Darüber hinaus können sich extern bedingte Wissensdiffusionen durch Reverse Engineering, Diebstahl, Abhören und Angriffe auf IT-Systeme ergeben.

Analog zu Wissensverlusten bestehen auch zwischen den Einzelrisiken der Wissensdiffusion Interaktionen, die sich durch die Literatur absichern lassen. So kann beispielsweise Fehlverhalten die Erfolgswahrscheinlichkeit einer Aushorchung durch Dritte erhöhen, wenn die Mitarbeiter zu sorglos

sensitive Inhalte oder Zugangsdaten weitergeben (Humpert 2004, 17). Analoges gilt für die Erhöhung der Eintrittswahrscheinlichkeit von Diebstählen, wenn durch die Mitarbeiter z.B. mobile Endgeräte nicht entsprechend gesichert werden oder deren Aufenthaltsort für Dritte ersichtlich ist (BSI 2006, 693). Weiterhin kann Fehlverhalten der Mitarbeiter im Umgang mit Sicherheitstechnologien zur Folge haben, dass die Erfolgswahrscheinlichkeit von Angriffen auf IT-Systeme ansteigt, da auf diese Weise erforderliche Schwachstellen geschaffen werden (BSI 2006, 328).

Hinsichtlich der Definition von Prozessen können unzureichende Zugangs- und Zugriffskontrollen im Hinblick auf den Einsatz temporär beschäftigter Mitarbeiter, die Zusammenarbeit mit Partnern sowie eingeschleuste und angeworbene Mitarbeiter zur Folge haben, dass Personen dieser Gruppen von Wissen Kenntnis nehmen können, das ihnen aus Gründen der Vertraulichkeit nicht zugänglich sein sollte (Maier 1992, 37f; Liebeskind 1997, 656ff; Matusik, Hill 1998, 680ff; Liman 1999, 240). Dies betrifft in diesen beiden Fällen auch die Dynamisierung von Zugriffsrechten, da so nach Beendigung eines Arbeitsverhältnisses bzw. einer Kooperationsbeziehung nach wie vor Zugriff auf sensitive Inhalte bestehen und so eine Diffusion von Wissen erfolgen kann (Rogulla, Walther 2003a, 21). Schwächen in Bezug auf das Zugriffskontrollsystem (z.B. in der Form einer fehlenden Limitierung von Anmeldeversuchen) können ebenfalls die Erfolgswahrscheinlichkeit von Angriffen auf IT-Systeme erhöhen (BSI 2006, 626, 688). Weiterhin kann technisches Versagen von einzelnen Systemkomponenten oder gesamten IT-Systemen zur Folge haben, dass die IT-Sicherheit durch den Ausfall eines Sicherheitssystems eingeschränkt wird und so im Speziellen das Zugriffskontrollsystem nicht voll funktionsfähig ist und folglich unautorisierte Zugriffe gewähren (BSI 2006, 632f). Darüber hinaus können erfolgreich eingeschleuste bzw. angeworbene Mitarbeiter, die im Interesse Dritter handeln, die Eintrittswahrscheinlichkeit des Abhörens der Kommunikation erhöhen, da sie sich Zugang verschaffen können, um beispielsweise Wanzen etc. zu platzieren (Maier 1992, 37f; Liman 1999, 240).

Insgesamt ist eine gewisse unerwünschte Diffusion von Wissen in der Regel nicht vollkommen vermeidbar. So bestehen so genannte Spillover Effekte, die dadurch auftreten, dass Wissen transferiert bzw. veröffentlicht wird und andere Unternehmen daran partizipieren. Derartige Effekte treten dann auf, wenn Dritte von der Nutzung des Wissens nicht vollkommen ausgeschlossen werden können und sind nur schwer kontollierbar (Schwamborn 1994, 241f; Inkpen 2000, 1027; Teece 2000b, 134; Lev 2001, 33; Inkpen, Currall 2004, 595). Darüber hinaus kann eine Begrenzung der Diffusion auch dem Erfolg des Wissenstransfers entgegenstehen, wenn dadurch beispielsweise die Interaktion zwischen den Transferpartnern begrenzt wird bzw. der Transferprozess übersteuert wird. Diese Betrachtungen sind Gegenstand des Abschnitte 5.5.

5.5 Wissenstransfer

Im Rahmen dieses Abschnittes werden Wissensrisiken, die mit einem unzureichenden Transfer von Wissen einhergehen, erörtert und dabei den vier Ursachenkategorien Personen, Prozesse, Systeme und externe Faktoren zugeordnet.

5.5.1 Allgemeine Betrachtung

Der Wissenstransfer stellt einen bedeutenden Prozess im WM dar, weshalb dieses Konzept vergleichsweise umfassend in der Literatur behandelt wird. Nach einer prozessorientierten Sichtweise liegt dieser Arbeit folgendes Begriffsverständnis zugrunde.

> Unter Wissenstransfer wird der Prozess durch den Wissen zwischen einem Sender und einem Empfänger übermittelt wird verstanden, wobei abgrenzend zum Transfer von Informationen eine De- und Rekontextualisierung des Wissens erforderlich ist (Argote, Ingram 2000, 156ff; Child 2001, 661; Cummings 2003, 6, 20ff; Sun, Scott 2005, 75f).

Bei diesem Prozess ist es aus Sicht des Unternehmens erforderlich, dass die Übertragung von Wissen möglichst vollständig und für den Partner verständlich im Sinne von erfolgreich stattfindet. Wissensrisiken bezeichnen somit in diesem Zusammenhang Faktoren, die die erfolgreiche Übertragung von Wissen behindern. Dabei kann der Erfolg des Wissenstransfers auf verschiedene Arten bestimmt werden (Cummings, Teng 2003, 40f). So kann der Erfolg quantitativ anhand der Anzahl der Transfere in einem bestimmten Zeitraum ermittelt werden. Unter Projektmanagementbezug kann der Wissenstransfer dann als erfolgreich angesehen werden, wenn zeitliche Vorgaben sowie Budgets eingehalten und Kundenzufriedenheit erreicht wurden Als weitere Variante kann der Erfolg des Wissenstransfers am Ausmaß der erfolgreichen Replikation des Wissens beim Empfänger festgemacht werden. Da Wissen an verschiedene Träger gebunden ist und das zu transferierende Wissen auf mehrere Träger verteilt sein kann, ist die Replikation schwer zu bewerten. Zudem kann der Wissenstransfer bei Anwendung eines Internalisierungsansatzes dann als erfolgreich angesehen werden, wenn der Empfänger Eigentümerschaft erlangt, vom transferierten Wissen überzeugt und mit diesem zufrieden ist (Cummings, Teng 2003, 40f; Pedersen et al. 2003, 83). Dabei weisen die verschiedenen Ansätze jeweils Vorzüge und Nachteile auf. So reicht die Bestimmung der Anzahl der Transfere nicht aus, da sie keinen Aufschluss über die Qualität des Wissenstransfers gibt. Das Ausmaß der Replikation selbst ist aufgrund der Bindung von Wissen an verschiedene Träger schwer bestimmbar. Zufriedenheit mit dem transferierten Wissen ist ebenso schwer zu generalisieren. Aus diesem Grund wird in diesem Kontext Wissenstransfer bei Erfüllung mehrerer Kriterien als erfolgreich angesehen. Zur Operationalisierung

des Wissenstransfererfolgs geeigneter erscheint in diesem Kontext die Berücksichtigung eines Anwendungsbezugs des Wissens. Dieser kann beispielsweise als Beitrag des transferierten Wissens zur Durchführung von Aufgaben, Prozessen oder Projekten angegeben werden (Simonin 1999, 621). Dabei betrifft der Wissenstransfererfolg zwar den gesamten Prozess und die beteiligten Akteure, kann jedoch primär an der Einschätzung des Empfängers festgemacht werden. Dieser beurteilt den Wissenstransfer neben dem Anwendungsbezug anhand weiterer Kriterien wie Qualität und Quantität des transferierten Wissens, Beitrag zur Erweiterung der Wissensbasis oder Reduktion von Abhängigkeiten vom Wissen des Partners im Verlauf der Partnerschaft (Wathne et al. 1996, 75; Simonin 1999, 621; Cummings, Teng 2003, 40f).

Wissenstransfer kann in internen und externen Transfer über die Organisationsgrenzen hinweg unterschieden werden (Szulanski 1996, 27; Dixon 2000, 144ff; Jacob, Ebrahimpur 2001, 77; Song et al. 2003, 352). Im vorliegenden Kontext wird primär auf den externen Wissenstransfer fokussiert, da er einerseits eine bedeutende Quelle für den Wissenserwerb darstellt und andererseits ein vergleichsweise höheres Risikopotential aufweist, das sich aus der Dualität zur Wissensdiffusion ergibt (Badaracco 1991, 123; Grant, Baden-Fuller 1995, 17ff; Husman 2001, 3; Escribá-Esteve, Urra-Urbieta 2002, 331). Wissenstransfer in Kooperationen ist vorwiegend auf der Ebene der operativen Geschäftsprozesse angesiedelt, da v.a. Mitarbeiter des mittleren Managements oder Ingenieure im Tagesgeschäft in Interaktion mit Mitarbeitern des Kooperationspartners stehen (Baughn et al. 1997, 104).

Dem unternehmensinternen Wissenstransfer, der nachfolgend nicht ausgeklammert, sondern sekundär betrachtet wird, kommt im Hinblick auf die Verbreitung von Wissen oder der effizienten Bewirtschaftung der Ressource Wissen eine Schlüsselrolle zu, da so beispielsweise erfolgreiche Konzepte repliziert[172] oder Doppelarbeiten vermieden werden können. Der Wissenstransferprozess weist Unterschiede auf, wenn er auf der Ebene von Individuen, Gruppen oder Unternehmen betrachtet wird. In Abhängigkeit der Ähnlichkeit der Aufgaben und des Kontexts, der Art der Aufgaben in Bezug auf Häufigkeit und Routinisierung sowie des Typs an zu transferierendem Wissen unterscheiden sich auch die Prozesse des Wissenstransfers (Dixon 2000, 144ff)[173].

[172] Im Rahmen der Verbreitung von Wissen wird auch vielfach von Replikation gesprochen. Winter und Szulanski diskutieren beispielsweise die Replikation von Routinen auf andere Abteilungen oder Filialen (Winter, Szulanski 2001, 730ff).

[173] Dixon unterscheidet zwischen serial, near, far und expert transfer, die sich jeweils aus den unterschiedlichen Ausprägungen dieser Faktoren ergeben (Dixon 2000, 144ff).

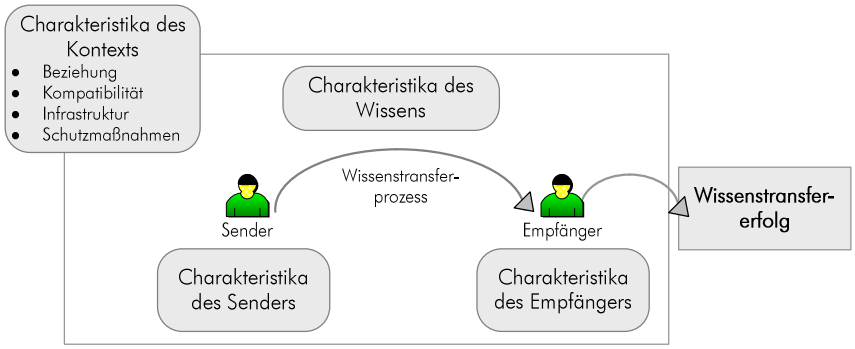


Abb. 24 Einflussfaktoren auf den Erfolg des Wissenstransfers

Der Erfolg des Wissenstransfers wird von einer Reihe von Risiken beeinflusst, die verschiedenen Kategorien zugeordnet werden können (Szulanski 1996, 30f; Matusik 2002b, 608; Cummings, Teng 2003, 43ff). Das in Abb. 24 dargestellte Modell dient zur Strukturierung von Einflussfaktoren, wobei positive Ausprägungen zum Erfolg beitragen und negative Ausprägungen als Risiko zu interpretieren sind, da sie den Erfolg des Wissenstransfers hemmen. So nehmen einerseits Faktoren, die das Verhalten und die Fähigkeiten von Sender und Empfänger im Umgang mit dem transferierten Wissen bzw. dem Partner betreffen, Einfluss auf den Erfolg des Wissenstransfers. Dabei wird der Erfolg des Wissenstransfers seitens des Senders beispielsweise durch dessen Motivation, Fähigkeit Wissen zu explizieren bzw. zu dekontextualisieren und dessen Verlässlichkeit beeinflusst (Lei 1993, 36; Szulanski 1996, 31; Larsson et al. 1998, 291; Husman 2001, 6; Fauchart 2003, 12; Maier 2004, 130).

Seitens des Empfängers beeinflussen dessen Motivation, Fähigkeit zur Wissensaufnahme und -bewahrung[174] sowie Vermeidungshaltungen in Bezug auf bestimmtes Wissen oder dem Sender gegenüber den Wissenstransfererfolg (Schüppel 1996, 124ff; Szulanski 1996, 31). Begriffe wie komplementäre Fähigkeiten beziehen sich ebenso auf dieses Konzept und beschreiben die Fähigkeit, externes Wissen zu integrieren (Badaracco 1991, 52ff; Kogut, Zander 1992, 391). Im Hinblick auf die Charakteristika des transferierten Wissens beeinflussen u.a. der Grad der Explizierung, die Spezifität, die Komplexität und die Kontexteinbettung des transferierten Wissens den Wissenstransfererfolg, da sie die Replikation beim Empfänger erschweren können. So beeinflussen eine geringe Explizierung und hohe Ausprägungen der anderen drei Charakteristika die Replikation negativ und stellen somit Risiken dar (Badaracco 1991, 47; Child, Faulkner 1998, 661; Matusik, Hill 1998, 687; Argote, Ingram 2000, 158; Jacob, Ebrahimpur 2001, 84; Parise, Henderson 2001, 910; Cummings, Teng 2003, 44; Soekijad, Andriessen 2004, 4)[175].

Einflussfaktoren der Kategorie Kontext betreffen die Umfeldbedingungen der Kooperationsbeziehung im Allgemeinen und des Wissenstransfers im Speziellen. Dabei ist zum einen die Beziehung zwischen den Partnern als Unterkategorie von Relevanz. Zum Zweiten weisen die Partner im Hinblick auf ihre

[174] Diese Fähigkeiten werden durch das Konzept der Absorptive Capacity beschrieben, unter das die Fähigkeiten externes Wissen zu akquirieren, zu assimilieren und anzuwenden subsumiert werden. Dabei ergibt sich diese organisatorische Fähigkeit aus den Einzelfähigkeiten der Mitarbeiter (Cohen, Levinthal 1990, 499ff). Eine weitere Verfeinerung des Konzeptes in Sub-Fähigkeiten wird durch Zahra und George vorgenommen (Zahra, George 2002, 189f).

[175] Für Details zu den Charakteristika von Wissen siehe Abschnitt 2.2.4.

Wissensbasen sowie ihre organisatorischen und soziokulturellen Besonderheiten Unterschiede bzw. Ähnlichkeiten auf, die den Wissenstransfererfolg negativ und positiv beeinflussen können. Zudem kommt der Infrastruktur sowohl aus technischer als auch aus institutioneller Sicht ein besonderes Gewicht zu. Da die Beziehungen zwischen den Partnern auch von Ver- bzw. Misstrauen geprägt sind, werden auch Schutzmaßnahmen ergriffen, um der ungewollten Diffusion von Wissen entgegenzuwirken. Diese Kategorie wird umfassender betrachtet, da sie im Hinblick auf die Steuerung von Wissensrisiken als Hauptuntersuchungsgegenstand der Arbeit aufgrund des Gestaltungsspielraums von Relevanz ist.

Beziehung: Die Unterkategorie Beziehung wird einerseits durch den Grad an Wettbewerb bestimmt, der sich beispielsweise aus der Ähnlichkeit der Geschäftsbereiche oder der Überlappung von Produkten und Kunden ergibt. Andererseits verfolgen die Partner auch unterschiedliche Ziele in Bezug auf die Aneignung von Wissen im Rahmen der Kooperation. Diese können vom bloßen Zugang bis hin zur Internalisierung des Wissens reichen (Hamel 1991, 90f; Baughn et al. 1997, 106; Mohr, Sengupta 2002, 291ff). Dabei unterscheiden sich verschiedene Partner darin, wie aggressiv sie diese Ziele zu erreichen versuchen und verhalten sich eventuell opportunistisch. Es kann angenommen werden, dass opportunistisches Verhalten jeder Kooperation inhärent ist, allerdings dieses Potential unterschiedlich genutzt wird, da beispielsweise negative Konsequenzen in der Branche befürchtet werden (Das 2005, 707). Opportunistisches Verhalten wird beispielsweise durch Reputationsdruck in der Branche oder durch die Existenz von Vertrauen zwischen den Partnern reduziert. Vertrauen nimmt zudem einen positiven Einfluss auf die Bereitschaft zum Wissenstransfer und dessen Gegenseitigkeit (Gulati et al. 2000, 209; Kale et al. 2000, 222)[176]. Besteht Vertrauen zwischen den Partnern so ist davon auszugehen, dass Schwachstellen eines Partners nicht vom anderen ausgenutzt werden (Mayer et al. 1995, 712; Inkpen, Currall 2004, 588). Geringer Wettbewerb, geringe Internalisierungsabsichten und starkes Vertrauen beeinflussen den Wissenstransfer zwischen den Partnern positiv und limitieren opportunistisches Verhalten, bergen aber andererseits Risikopotentiale in sich.

Kompatibilität: Die Unterkategorie Kompatibilität bezieht sich auf die Unterschiede im Hinblick auf Organisation, Kultur und Wissensbasen der Partner. Unterschiede bzw. Ähnlichkeiten in Bezug auf die Organisation betreffen beispielsweise Geschäftsfelder, Größenklassen, Geschäftspraktiken oder die Unternehmenskultur (Simonin 1999, 603; Szulanski et al. 2003, 144f), während hinsichtlich Kultur Unterschiede der Sprache oder kultureller Normen und Praktiken den Wissenstransfer beeinflussen, wobei diese Faktoren insbesondere in internationalen Kooperationen stärker zum Tragen kommen (Simonin 1999, 602; Lane et al. 2001, 1143f). Darüber hinaus nimmt die Ähnlichkeit der Wis-

[176] Besteht das Ziel der Internalisierung und wird zugleich opportunistisches Verhalten zur Erreichung dieses Ziels in Kauf genommen, so spricht man auch oftmals vom Outlearning, also der vollständigen Absorbierung der Kompetenzen des Partners. Damit verbunden sind auch vielfach so genannte Lernrennen, mittels derer so schnell als möglich das Wissen des Partners absorbiert werden soll (Gulati et al. 2000, 209; Kale et al. 2000, 217; Soekijad, Andriessen 2004, 3).

sensbasen Einfluss auf den Wissenstransfererfolg. Dabei können Lücken in Bezug auf bestimmte Kompetenzen die Rekontextualisierung des Wissens erschweren, sogar unmöglich machen und somit Risikopotentiale in sich bergen (Hamel 1991, 91; Cummings, Teng 2003, 46f; Song et al. 2003, 355). Geringere Unterschiede der Partner im Hinblick auf diese drei Ebenen tragen positiv zum Wissenstransfererfolg bei, während mit zunehmenden Unterschieden die Risikopotentiale steigen (Matusik 2002b, 613).

Infrastruktur: Weitere Einflussfaktoren im Bereich des Kontexts lassen sich anhand der Unterkategorie Infrastruktur beschreiben. Diese betrifft die organisatorische und technische Unterstützung der Zusammenarbeit. Räumliche Nähe zwischen den Wissenstransferpartnern beeinflusst den Transfer von Wissen v.a. durch die Ermöglichung des persönlichen Kontakts positiv. Die räumliche Nähe kann bereits aufgrund geographischer Lagen gegeben sein oder gezielt durch die Einrichtung gemeinsamer Produktionsstandorte oder die Rotation von Mitarbeitern erfolgen. Dadurch wird die Beobachtbarkeit des Wissens erhöht (von Krogh, Roos 1996, 35ff; Loebbecke et al. 1999, 35ff; Teece 2002, 14; Cummings, Teng 2003, 46). Neben der räumlichen Nähe ist auch eine möglichst umfassende Zahl an Interaktionskanälen, die sowohl technischen als auch organisatorischen Charakter aufweisen können, für den Erfolg des Wissenstransfers förderlich, wobei dies im Hinblick auf die Diffusion von Wissen (siehe Abschnitt 5.4) aufgrund der erschwerten Kontrollierbarkeit Risikopotentiale in sich birgt (Hamel et al. 1989, 136; Maier 2004, 127; Schmaltz et al. 2004, 3f). Diese Interaktionskanäle werden auch zum Teil als Wissenstransfermechanismen bezeichnet und können formeller und informeller Natur sein. Sie umfassen beispielsweise persönlichen Austausch, gemeinsame Datenbanken, Communities, gemeinsame Technologienutzung, gemeinsame Projektteams oder Einsatz von Groupware (Dyer, Nobeoka 2000, 352ff; Inkpen 2000, 1031; Almeida et al. 2002, 158; Becker, Knudsen 2003, 22; Cummings, Teng 2003, 63; Strach, Everett 2006, 64). Zudem können verschiedene geteilte Technologien oder Verfahrensweisen sowie die organisatorische Rolle eines Brückenbauers[177] ein gemeinsames Verständnis fördern und so positiv zum Wissenstransfererfolg beitragen (Brown, Duguid 1998, 104; Awazu 2004b, 18f; Haider, Mariotti 2004, 5f).

Schutzmaßnahmen: Im Hinblick auf den Trade-off zwischen Ermöglichung erwünschter Transferprozesse und Verhinderung einer unerwünschten Diffusion von Wissen kommt den ergriffenen Schutzmaßnahmen eine bedeutende Rolle zu. Mit zunehmendem Überschreiten von Abteilungs- und Unternehmensgrenzen nehmen die Barrieren in Bezug auf den Wissenstransfer und die Angst vor Kontrollverlust zu (Jacob, Ebrahimpur 2001, 84; Sun, Scott 2005, 80). Geht man davon aus, dass sich die Mitarbeiter im operativen Tagesgeschäft oftmals unsicher sind, ob Wissen an den Partner weitergegeben werden kann oder nicht, so kann davon ausgegangen werden, dass Wissenstransferrichtlinien den Erfolg des Wissenstransfers erhöhen, da sie Klarheit schaffen, Zurückhaltung von eigentlich

[177] Diese Rolle wird auch als Boundary Spanner bezeichnet (Maier 2004, 146).

transferierbarem Wissen verhindern und so einen offeneren Umgang mit Wissen ermöglichen (Jordan, Lowe 2004, 256). Zu beachten ist in diesem Kontext allerdings, dass eine Überklassifikation des Wissens erwünschte Wissenstransferprozesse verkomplizieren und somit hemmen kann (Desouza, Vanapalli 2005, 80). Zudem können beispielsweise mittels IT-Sicherheitsrichlinien Anforderungen an die Wissenstransferprozesse gestellt werden oder über Gatekeeper oder Kooperationsbüros die organisationsübergreifenden Transferprozesse kontrolliert bzw. genehmigt werden (Hamel et al. 1989, 136; Fleischer 1997, 238; Awazu 2004b, 19). Dabei ist aber zu beachten, dass eine derartige Kontrolle der Mitarbeiter Misstrauen signalisieren und dies negative Effekte auf deren Leistung haben kann (Maier 1992, 102). Ferner können zwischen den Partnern Kooperationsvereinbarungen auf der Basis von Verträgen getroffen werden, die beispielsweise regeln, welches Wissen ausgetauscht wird, inwieweit es außerhalb der Kooperation nutzbar ist und ob es an Dritte transferiert werden kann (Lei 1993, 36; Liebeskind 1997, 632; de Laat 1999, 209; Loebbecke et al. 1999, 20). In allen diesen Fällen ist zu beachten, dass derartige Regulierungen Barrieren aufbauen, die den Wissenstransfererfolg negativ beeinträchtigen können und somit Wissensrisikopotentiale darstellen. Zudem kann die Einforderung vertraglicher Vereinbarungen Misstrauen signalisieren und dies die Beziehung zwischen den Partnern negativ beeinträchtigen (Woolthuis et al. 2002, 3). Somit ist insbesondere bei Schutzmaßnahmen, von denen im Gegensatz zu den anderen Kontextfaktoren ein Handlungspotential ausgeht, stets zu beachten, dass zwar einerseits unerwünschte Prozesse im Bereich der Diffusion von Wissen gehemmt werden, aber diese Hemmung nicht zugleich die erwünschten Wissenstransferprozesse zu stark beeinträchtigt.

5.5.2 Einzelrisiken

Personen: Risiken dieser Kategorie stehen im primären Ursachenkontext von Personen, was bedeutet, dass sie auf das Verhalten, Handlungen oder mangelnde Kompetenzen der Mitarbeiter zurückgeführt werden können.

- **Zurückhaltung aufgrund Unsicherheit (TP1)**: Im Hinblick auf den Wissenstransfer speziell mit externen Partnern bestehen vielfach Unsicherheiten, inwiefern Wissen weitergegeben werden kann oder nicht. Während eine zu freigebige Weitergabe von Wissen mit dem Risiko einer unerwünschten Diffusion einhergehen kann, kann im umgekehrten Fall, also einer sehr restriktiven Handhabung, das Risiko bestehen, dass eigentlich transferierbares Wissen zurückgehalten wird und so Potentiale des Wissenstransfers nicht genutzt werden (Jordan, Lowe 2004, 256). Eine derartige Zurückhaltung kann die Weiterentwicklung des Wissens oder die Gegenseitigkeit des Wissenstransfers negativ beeinträchtigen und stellt somit ein Risiko dar.
- **mangelndes Vertrauen (TP2)**: Neben der Zurückhaltung aufgrund von Unsicherheiten kann auch mangelndes Vertrauen gegenüber dem Transferpartner ein Risiko darstellen, das sich negativ auf

den Wissenstransfererfolg auswirkt. Misstrauen kann sich im unternehmensübergreifenden Fall u.a. aus einer Konkurrenzsituation der Unternehmen, Angst vor Übernahme oder Zusammenarbeit mit ehemaligen Konkurrenten ergeben, während im unternehmensinternen Fall die Angst vor Ersetzbarkeit herangezogen werden kann (Schüppel 1996, 152; Lück, Schulte 1997, 666f; Riege 2005, 23). Neben der Weitergabe von Wissen beeinflusst mangelndes Vertrauen auch die Bereitschaft zur Aufnahme bestimmten Wissens. Ist die Verlässlichkeit des Partners gering oder weist er eine geringe Reputation auf, so hemmt dies die Annahme des Wissens und somit die Wissenstransferprozesse (Szulanski 1996, 31).

- **Abwehr- / Vermeidungshaltung (TP3)**: Ein Wissensrisiko kann darin bestehen, dass Mitarbeiter eine Abwehr- bzw. Vermeidungshaltung gegenüber Wissen aus externen oder internen Quellen haben und sich dies hemmend auf den Wissenstransferprozess auswirkt, da erforderliches Wissen potentiell nicht in erwünschtem Umfang bzw. in entsprechender Qualität vorliegt. Eine derartige Abwehr- bzw. Vermeidungshaltung kann verschiedene Ursachen haben und auf Wettbewerb zwischen Abteilungen, Projekten oder Unternehmen sowie auf persönliche Differenzen zurückgehen (Schüppel 1996, 162ff; Riege 2005, 23ff). Neben spezifischen interpersonellen Konflikten kann eine Person generell eine Vermeidungshaltung gegenüber Innovationen bzw. Veränderungen haben und dadurch der Erfolg des Wissenstransfers negativ beeinträchtigt werden.
- **unzureichende Explizierung (TP4)**: Ein unzureichender Transfer kann auch dadurch hervorgerufen werden, dass den am Wissenstransfer beteiligten Mitarbeitern entsprechende Kompetenzen fehlen bzw. nicht in ausreichendem Maße vorhanden sind. So können Kompetenzen zur Explizierung und Dekontextualisierung von Wissen unzureichend sein und durch eine erschwerte Anwendbarkeit beim Partner der Erfolg des Wissenstransfers gemindert werden (Larsson et al. 1998, 291; Husman 2001, 6).
- **unzureichende Absorbierung (TP5):** Neben einer unzureichenden Explizierung von Wissen sind auch Kompetenzen in Bezug auf die Aufnahme von Wissen erforderlich, die beispielsweise dessen Dekontextualisierung, Interpretation und Adaption einschließen. Diese Fähigkeit wird auch als Absorptive Capacity bezeichnet, wobei dieses Konzept eine organisatorische Fähigkeit beschreibt, die sich aus der Aggregation der Einzelfähigkeiten der Mitarbeiter ergibt (Cohen, Levinthal 1990, 499ff). Die Absorptive Capacity und die Zugänglichkeit des Wissens des Partners, die durch das Schutzverhalten des Partners bestimmt wird, machen die Lernfähigkeit aus (Baughn et al. 1997, 107). Sind diese Kompetenzen unzureichend, besteht das Risiko, dass der Transfererfolg gemindert wird, da der Grad der Replikation des transferierten Wissens beim Empfänger reduziert wird.

Prozesse: Risiken im Hinblick auf einen unzureichenden Transfer der Kategorie Prozesse können auf organisatorisch zu verantwortende Schwächen der Rahmenbedingungen, in denen der Wissenstrans-

ferprozess stattfindet, zurückgeführt werden. Diese sind Gegenstand der nachfolgenden Sammlung an Risiken.

- **unbegleitete Reorganisation (TO1)**: Wissenstransferprozesse können Reorganisation (siehe auch VO1) und Reengineering negativ beeinträchtigen. So werden bedingt durch die Fluktuation der Mitarbeiter zu anderen Unternehmen etablierte und zum Teil informelle Strukturen des Wissenstransfers aufgebrochen. Auch im Falle der Intrafluktuation können die Wissenstransferprozesse negativ beeinträchtigt werden, da insbesondere die Einbindung in informelle Strukturen verloren gehen kann. Ebenfalls einen negativen Einfluss kann das Reeingeneering von Prozessen, das mit einer Straffung der Abläufe einhergeht, haben, da Spielräume für Wissenstransfer und Wissensentwicklung wegfallen können (Knaese 2004, 52; Probst et al. 2006, 66).
- **unbegleitete Beendigung von Projekten (TO2)**: Ebenso wie die Reorganisation können auch durch das Projektgeschäft die Wissenstransferprozesse negativ beeinträchtigt werden. So werden durch die unbegleitete bzw. reaktive Beendigung von Projekten und der damit einhergehenden räumlichen Umverteilung der Mitarbeiter etablierte Strukturen aufgelöst, was zur Folge haben kann, dass persönliche[178] unternehmensinterne und -externe Beziehungen oftmals nur schwer aufrechtzuerhalten sind. Doch gerade auch persönliche und informelle Beziehungen sind für Wissenstransferprozesse von Bedeutung (Schindler 2001, 68; Burghardt 2002, 91; Disterer 2002, 512; Schindler, Eppler 2003, 220). Zudem kann die zentrale und dezentrale Arbeitsteilung in Projekten Informationslücken zur Folge haben und somit ebenfalls die Wissenstransferprozesse hemmen (Schön 2004, 287). Wenn Beziehungen zwischen den Mitarbeitern sowie Stakeholdern des Projektes verloren gehen, geht dies mit einer Reduktion des Beziehungskapitals (siehe Abschnitt 2.3.1) einher.
- **fehlende Transparenz über vorhandenes Wissen (TO3)**: Der Wissenstransfer kann im unternehmensinternen und -externen Fall dadurch negativ beeinträchtigt werden, dass nicht transparent ist, mit welchen Themen sich Mitarbeiter anderer Teams, Abteilungen, Projekte oder Partner beschäftigen und welches Wissen in welcher Form zu diesen Themen vorhanden ist. Dieses Risiko wird vielfach dadurch hervorgerufen, dass Schnittstellen fehlen bzw. unzureichend definiert sind. Auf diese Weise kann es beispielsweise zu einer Nichtbeachtung von Vorgängerprojekten, ungeeigneten Übergaben zwischen Teams oder Mitarbeitern der Kooperationspartner kommen (Keßler, Winkelhofer 2002, 162; Schön 2004, 288). Dies hat zur Folge, dass Wissen, das eigentlich vorhanden wäre, für die Durchführung bestimmter Aufgaben erneut entwickelt wird.
- **eingeschränkte Zusammenarbeit (TO4)**: Während von einer intensiven interorganisatorischen Zusammenarbeit mit Partnern Risiken der Diffusion ausgehen (siehe DO4), da die Kontrollierbar-

[178] Virtuell können Beziehungen aufrechterhalten werden. Jedoch sind persönliche Beziehungen dem Wissenstransfer förderlich und insbesondere beim Transfer von implizitem Wissen mit einer hohen Komplexität überlegen. Siehe hierzu auch die Anmerkungen zur Kategorie Infrastruktur in Abschnitt 5.5.1.

keit der Interaktionen bedingt durch die zunehmende Anzahl erschwert wird, setzt ein erfolgreicher Transfer von Wissen gerade eine intensive Zusammenarbeit z.B. durch die Bildung gemeinsamer Teams oder die Rotation von Personal voraus. Dies ist insbesondere dann der Fall, wenn komplexes, vorwiegend implizites Wissen, das schwer formalisierbar und artikulierbar ist, transferiert werden soll (Mohr, Sengupta 2002, 285; Cummings, Teng 2003, 46; Pedersen et al. 2003, 83; Lang 2004, 91f). Einschränkungen in diesen Bereichen bergen somit das Risiko in sich, dass der Wissenstransfererfolg abnimmt bzw. die Potentiale des Wissenstransfers nicht genutzt werden. Auch im unternehmensinternen Fall kann eine Einschränkung der Zusammenarbeit aus Gründen der Sicherheit erfolgen und analoge Risikopotentiale in sich bergen (Maier 2004, 130; Riege 2005, 25ff)[179].

- **hemmende Sicherheitsrichtlinien (TO5)**: Auch interorganisatorische Wissenstransferprozesse können aufgrund zu rigider Sicherheitsrichtlinien in Bezug auf die Nutzung von IT-Systemen (z.B. Verschlüsselung) oder sonstigen organisatorischen Maßnahmen wie den Einsatz von Gatekeepern oder Kooperationsbüros, die den externen Wissenstransfer kontrollieren, ebenso wie von einer Überklassifizierung des Wissens gehemmt werden (Fleischer 1997, 238; Mahnke 1999, 8; Desouza, Vanapalli 2005, 87f). So kann die Überwachung der Wissenstransferprozesse und der entsprechende Einsatz von Kontrollmaßnahmen zur Folge haben, dass das Vertrauen der Mitarbeiter sinkt, da sie davon ausgehen, dass ihnen misstraut wird oder der Transfer bedingt durch den erhöhten Zeitaufwand unterbleibt (Liebeskind 1997, 637f). Im Speziellen können auch vertragliche Vereinbarungen im Rahmen von Kooperationen potentiell eine hemmende Wirkung aufweisen, da sie ebenfalls Misstrauen beim Partner erzeugen können (Husman 2001, 19; Oliver 2004, 163).
- **Inkompatibilität zwischen den Partnern (TO6)**: Wissensrisiken können sich im Rahmen von Kooperationen daraus ergeben, dass Inkompatibilitäten zwischen den Partnern bestehen und dadurch der Erfolg bzw. die Potentiale des Wissenstransfers gehemmt werden. Inkompatibilitäten können dabei die Strategien der Partner, deren organisatorische Besonderheiten, deren soziokulturelle Charakteristika sowie Unterschiede im Hinblick auf die Kompetenzen und die Wissensbasen betreffen. Hinsichtlich der Strategie kann es der Fall sein, dass kein Fit vorliegt oder die Strategien sogar zueinander im Konflikt stehen (Gahl 1991, 53). Hemmende Faktoren im Bereich Organisation können sich beispielsweise aus Inkompatibilitäten im Hinblick auf Geschäftspraktiken oder Unternehmenskulturen ergeben (Simonin 1999, 603; Szulanski et al. 2003, 144f). Zudem können sich auch Inkompatibilitäten im soziokulturellen Bereich, wie z.B. Sprachbarrieren oder unterschiedliche kulturelle Normen, hemmend auf den Erfolg des Wissenstransfers auswirken (Gahl

[179] So können z.B. starre hierarchische Machtstrukturen, die Begrenzung informeller Freiräume, die Unterbindung direkter Kommunikationswege, ebenso wie Wettbewerb zwischen den Abteilungen einen effizienten Wissenstransfer behindern. Siehe hierzu auch (Riege 2005).

1991, 53; Simonin 1999, 602; Lane et al. 2001, 1143f; Stanek 2004, 188f). Aus einer wissensorientierten Perspektive kann der Wissenstransfererfolg insbesondere durch Inkompatibilitäten der Kompetenzen oder Wissensbasen der Partner reduziert werden (Hamel 1991, 91; Hill, Hellriegel 1994, 594; Nielsen 2002, o.S.; Cummings, Teng 2003, 46f; Song et al. 2003, 355).

Systeme: Ein unzureichender Transfer kann auch darauf zurückzuführen sein, dass die IT eine ungeeignete Unterstützung darstellt oder sogar aufgrund zu hoher Komplexität, eines zu hohen Zeitaufwands oder geringer Akzeptanz einen Wissenstransfer hemmenden Faktor darstellt.

- **Bereitstellung unzureichender Medien (TS1):** Wissenstransferprozesse innerhalb des Unternehmens oder unternehmensübergreifend mit Partnern werden vielfach technisch unterstützt. Insbesondere bei implizitem und komplexem Wissen ist allerdings ein persönlicher Wissensaustausch dem technisch gestützten virtuellen Wissensaustausch überlegen. In Abhängigkeit von den Charakteristika des zu transferierenden Wissens steigt der Bedarf an ein reichhaltiges Medium[180] (Husman 2001, 10; Almeida et al. 2002, 158). Bedingt durch die Dislozierung der Wissenstransferpartner und des Zeit- und Kostenaufwandes für persönliche Treffen, erfolgt der Wissenstransfer vielfach virtuell (Pedersen et al. 2003, 76). In diesem Fall können sich Risiken im Hinblick auf die Hemmung des Wissenstransfers daraus ergeben, dass die technische Unterstützung unzureichend oder ungeeignet ist.
- **unzureichende Anwenderfreundlichkeit (TS2)**: Neben fehlendem Medienreichtum kann auch die Anwenderfreundlichkeit der zur Verfügung stehenden technischen IT-Systeme zu gering sein und somit Wissenstransferprozesse hemmen. So kann eine fehlende Integration der IT-Systeme und der Prozesse ebenso wie deren mangelnde Kompatibilität und Orientierung an den Bedürfnissen der Nutzer die Wissenstransferprozesse hemmen, indem die erforderliche Unterstützung nicht geboten wird. Zudem kann die Nutzung der IT-Systeme mit einem hohen zeitlichen Aufwand verbunden sein und somit deren Akzeptanz gering sein. Dies kann zur Folge haben, dass die Nutzung unterbleibt (Riege 2005, 29f).
- **unzureichende Vertrauenswürdigkeit (TS3)**: Ein effizienter Wissenstransfer setzt auch voraus, dass die zu dessen Unterstützung eingesetzten IT-Systeme eine hohe Vertrauenswürdigkeit aufweisen. Wird deren Sicherheit als zu gering erachtet oder wird deren Verlässlichkeit als zu gering eingeschätzt, kann Vertrauen in diese Systeme fehlen und somit die Akzeptanz und Nutzung negativ beeinträchtigt werden (Riege 2005, 29f)[181].

externe Faktoren: Neben internen Ursachen der Kategorien Personen, Prozesse und Systeme kann ein unzureichender Transfer auch auf externe Faktoren zurückgeführt werden, denen die nachfolgend erörterten Risiken zugeordnet werden können.

[180] Siehe hierzu auch die Media Richness Theorie (Daft, Lengel 1986).

[181] Riege fokussiert auf die Nichterfüllung von Anforderungen der Mitarbeiter. Diese kann im Speziellen auch die mangelnde Vertrauenswürdigkeit betreffen.

- **mangelnde Leistungsfähigkeit des Partners (TE1)**: Das und Teng unterscheiden in Kooperationen zwischen einem Beziehungs- und einem Leistungsrisiko. Während sich ersteres auf das potentielle opportunistische Verhalten des Kooperationspartners bezieht, betrifft das Leistungsrisiko dessen Leistung im Hinblick auf die in die Kooperation einzubringende Beiträge. Ein Leistungsrisiko hat somit zur Folge, dass der Erfolg der Kooperation bzw. des Wissenstransfers eingeschränkt ist (Das, Teng 1999, 51). Mangelnde Leistungsfähigkeit des Partners kann zudem eine Unausgewogenheit der Kooperation bedingen und deren Beendigung nach sich ziehen.
- **mangelnde Leistungsbereitschaft des Partners (TE2)**: Während sich mangelnde Leistungsfähigkeit des Partners auf ein Nichtkönnen zurückführen lassen, kann in einer mangelnden Leistungsbereitschaft ein Risiko gesehen werden, das im Zusammenhang mit Nichtwollen und opportunistischem Verhalten steht. So kann Trittbrettfahrerverhalten des Partners den Erfolg des Wissenstransfers mindern, wobei die Eintrittswahrscheinlichkeit dieses Risikos vergleichsweise geringer ist, wenn die zu leistenden Beiträge leicht kontrollierbar sind. Ist dies nicht der Fall, besteht mehr Raum für derartiges Verhalten (Fleischer 1997, 242). Ebenso beeinflusst auch die Qualität und Quantität des transferierten Wissens die Leistungsbereitschaft des Partners. Wird dieses als unausgewogen oder unzureichend interpretiert, so steigt die Wahrscheinlichkeit, dass die Leistungen durch den Partner reduziert werden.
- **Schutzverhalten des Partners (TE3)**: Ebenso wie unternehmenseigene Schutzmaßnahmen den Wissenstransfer hemmen können, kann auch das Schutzverhalten des Partners zu einer Einschränkung des zum Transfer zur Verfügung stehenden Wissens oder der Interaktionskanäle führen (Simonin 1999, 601f). Zudem können Sicherheitsmaßnahmen, die beim Partner ergriffen werden, die Bereitschaft zum Wissenstransfer seitens der Mitarbeiter negativ beeinträchtigen. Dabei nimmt das Schutzverhalten in der Regel zu, wenn Team-, Abteilungs- und Unternehmensgrenzen überschritten werden und ist somit im Falle von Kooperationen oftmals ausgeprägter (Sun, Scott 2005, 80ff). Dabei ergeben sich die Lernmöglichkeiten für das Unternehmen einerseits aus der Zugänglichkeit zum Wissen des Partners, das von dessen Schutzverhalten abhängig ist, und andererseits vom Grad der Absorptive Capacity als Aggregat der Einzelfähigkeiten der am Wissenstransfer beteiligten Mitarbeiter (Baughn et al. 1997, 107). Ein ausgeprägtes Schutzverhalten des Partners kann somit trotz ausgeprägter organisatorischer Fähigkeiten die Potentiale und den Erfolg des Wissenstransfers begrenzen und somit einen Risikofaktor darstellen.

5.5.3 Diskussion

Betrachtet man die Wissensrisiken des Konzeptes Wissenstransfer zusammenfassend, so können den vier Kategorien Personen, Prozesse, Systeme und externe Faktoren Risiken zugeordnet werden, wobei die beiden erstgenannten Kategorien vergleichsweise stärker besetzt sind, da Wissenstransfer auf der

Ebene von Personen betrachtet wird und zudem ein prozessorientiertes Verständnis zugrunde liegt (siehe Tab. 10). Wissensrisiken, die der Kategorie Personen zugeordnet sind, betreffen auf der einen Seite personenbezogene Barrieren wie Unsicherheit, mangelndes Vertrauen oder Abwehrhaltung. Zum anderen werden dieser Kategorie auch Risiken zugewiesen, die durch mangelnde Kompetenzen im Zusammenhang mit der Explizierung beim Sender bzw. der Absorbierung beim Empfänger einhergehen. Wissenstransferrisiken der Kategorie Prozesse beziehen sich auf das Umfeld des Wissenstransfers und betreffen vorwiegend organisatorische Barrieren wie Reorganisation, Beendigung von Projekten, mangelnde Transparenz, eingeschränkte Zusammenarbeit, hemmende Sicherheitsrichtlinien oder Inkompatibilitäten zwischen den Partnern. Die Kategorie Systeme schließt diejenigen Wissensrisiken ein, die in Zusammenhang mit einer technischen Unterstützung des Wissenstransfers stehen und betreffen im Einzelnen die Bereitstellung unzureichender Medien, unzureichende Anwenderfreundlichkeit sowie unzureichende Vertraulichkeit. Im Gegensatz zum Konzept Wissensdiffusion, das dadurch charakterisiert ist, dass eine Vielzahl an Akteuren involviert sein kann, findet der Wissenstransfer zwischen einem Sender und Empfänger statt. Somit betreffen die externen Faktoren im unternehmensübergreifenden Fall den jeweiligen Partner. So betreffen die Risiken im Einzelnen die mangelnde Leistungsfähigkeit, die mangelnde Leistungsbereitschaft sowie Schutzverhalten des Partners. Ebenso wie bei den zuvor betrachteten Konzepten können aus der Literatur einige Interaktionen zwischen den dargestellten Einzelrisiken identifiziert werden.

Kategorie	No	Wissensrisiko
Personen	TP1	Zurückhaltung aufgrund Unsicherheit
	TP2	mangelndes Vertrauen
	TP3	Abwehr-/ Vermeidungshaltung
	TP4	unzureichende Explizierung
	TP5	unzureichende Absorbierung
Prozesse	TO1	unbegleitete Reorganisation
	TO2	unbegleitete Beendigung von Projekten
	TO3	fehlende Transparenz über vorhandenes Wissen
	TO4	eingeschränkte Zusammenarbeit
	TO5	hemmende Sicherheitsrichtlinien
	TO6	Inkompatibilitäten zwischen den Partnern
Systeme	TS1	Bereitstellung unzureichender Medien
	TS2	unzureichende Anwenderfreundlichkeit
	TS3	unzureichende Vertraulichkeit
externe Faktoren	TE1	mangelnde Leistungsfähigkeit des Partners
	TE2	mangelnde Leistungsbereitschaft des Partners
	TE3	Schutzverhalten des Partners

Tab. 10 Wissensrisiken der Kategorie Wissenstransfer

So kann beispielsweise die Zurückhaltung von Wissen durch einen Partner zur Folge haben, dass die Potentiale des Wissenstransfers nicht ausgenutzt werden und die Leistungsbereitschaft des Partners sinkt, da der Prozess durch Gegenseitigkeit gekennzeichnet ist (Larsson et al. 1998, 289f; Escribá-Esteve, Urra-Urbieta 2002, 340ff). Darüber hinaus kann mangelndes Vertrauen in den Partner zur Folge haben, dass Wissen durch die Mitarbeiter zurückgehalten wird, da sie befürchten, dass der Partner Schwachstellen zum Nachteil des Unternehmens nutzt (Kale et al. 2000, 221f). Weiterhin kann mangelndes Vertrauen zur Folge haben, dass zu dessen Substitution Kontrollen in der Form von rigideren Sicherheitsrichtlinien ergriffen werden. Durch diese Maßnahmen kann ebenfalls die Leistungsbereitschaft des Partners gehemmt werden (Larsson et al. 1998, 289;

Simonin 1999, 602; Norman 2004, 613; Stanek 2004, 186). Weiterhin können ergriffene Sicherheitsmaßnahmen auch zur Folge haben, dass der Partner als Reaktion sein Schutzverhalten ebenso erhöht und dadurch der Wissenstransfer weiter eingeschränkt wird, was sich negativ auf dessen Potentiale bzw. den Gesamterfolg auswirken kann (Norman 2004, 613). Hinsichtlich Risiken in Bezug auf den Wissenstransfer gilt es zu beachten, dass sich die Interaktionen vielfach auf Aktionen eines Partners und entsprechende Gegenreaktionen des anderen Partners beziehen. So kann das Potential des Wissenstransfers vergleichsweise schnell reduziert werden, indem beispielsweise als Reaktion auf das Ergreifen von Schutzmaßnahmen durch einen Partner, der andere Partner ebenfalls sein Schutzverhalten erhöht. Analoges gilt für die Zurückhaltung von Wissen aufgrund eines mangelnden Vertrauens und Unsicherheiten über dessen Transferierbarkeit, da ein Transfer in geringem Umfang auch zugleich die Leistungsbereitschaft des anderen Partners limitiert und somit die Potentiale des Wissenstransfers reduzieren kann.

Im Hinblick auf die verschiedenen Charakteristika, die in Abschnitt 5.5.1 dargestellt wurden, ist der Kontext des Wissenstransfers für dessen Erfolg relevant, da diese Dimension vergleichsweise stark beeinflussbar ist. Dabei ist insbesondere auch die Auswahl des Partners bzw. die Beziehung zum Partner entscheidend, da mit dieser eine Reihe von präventiv ausschließbaren bzw. reduzierbaren Risiken einhergehen[182]. So können durch eine entsprechende Partnerwahl Risiken in Bezug auf Inkompatibilitäten, mangelnde Leistungsfähigkeit oder Vermeidungshaltungen reduziert werden.

5.6 Wissensqualität

Im Rahmen dieses Abschnittes werden Wissensrisiken, die im Zusammenhang mit einer eingeschränkten Qualität von wissensbezogenen Ressourcen stehen, erörtert und dabei den generischen Ursachenkategorien zugeordnet. Risiken in Bezug auf die Wissensqualität beziehen dabei sowohl dokumentiertes Wissen als auch Kompetenzen der Mitarbeiter und die Qualität von Prozessen bzw. Routinen ein. Bei der Beurteilung der Qualität von Inhalten ist zu berücksichtigen, dass diese einer subjektiven Einschätzung durch die Mitarbeiter unterliegt. Da eine subjektive Beurteilung mit einer hohen Variabilität einhergeht und somit eine stark individualisierte Steuerung dieser Risiken erforderlich wäre, werden nachfolgend vorwiegend Risiken herangezogen, deren Erwartungswerte vergleichsweise weniger subjektiven Einflüssen unterliegen. Demnach können Risiken einerseits mit den Inhalten selbst und somit den Autoren bzw. den Prozessverantwortlichen im Zusammenhang stehen und andererseits die Medien, also die technische Infrastruktur und somit die jeweiligen IT-Administratoren betreffen (Eppler 2003c, 39).

[182] Für Details siehe hierzu auch (Lei 1993, 37; Inkpen, Currall 2004, 589).

5.6.1 Allgemeine Betrachtung

Qualität kann im Hinblick auf verschiedene Gegenstände definiert werden, wobei in diesem Kontext die Qualität von Wissen den zentralen Betrachtungsgegenstand bildet[183]. Diese wird zum aktuellen Zeitpunkt in der Literatur nur gering diskutiert, während zur Beurteilung der Qualität von Informationen eine Vielzahl an Ansätzen besteht. So unterscheidet Nohr zwischen konstruktiver und rezeptiver Informationsqualität. Während erstere Anforderungen an die Erstellung definiert, bezieht sich die rezeptive Informationsqualität auf bereits vorhandene und vielfach externe Informationen (Nohr 2001, 5f). Nach Huang et al. ist die Fokussierung auf die Nutzer der Information entscheidend. Somit müssen die Informationen „fit for use“ d.h. bedarfsgerecht sein bzw. die Erwartungen der Nutzer erfüllen oder sogar übertreffen (Huang et al. 1999, 49). Mantwill reflektiert Informationsqualität vor dem Hintergrund verschiedener Kategorien von Gütern. So lassen sich Suchgüter vor dem Kauf qualitativ beurteilen, während die Qualität von Erfahrungsgütern erst nach dem Kauf bestimmt werden kann. Als dritte Kategorie bestehen Vertrauensgüter, deren Qualität weder vor noch nach dem Kauf vollständig bewertet werden kann. Informationen stellen nie Suchgüter dar, sondern fallen in die beiden letztgenannten Kategorien. Verfügen die Nutzer der Information über Informationskompetenz, so ist eine nachträgliche Beurteilung wie im Falle von Erfahrungsgütern möglich, während mit abnehmender Informationskompetenz eine Beurteilung der Qualität erschwert wird und folglich Informationen als Vertrauensgüter zu kategorisieren sind (Mantwill 1995, 46ff). Aufgrund dieser Eigenschaften von Informationen ist es bedeutend, dass die Nutzer über eine entsprechende Informationskompetenz verfügen, um die Qualität der Informationen beurteilen zu können. Bei der Beurteilung der Qualität ist allgemein zu beachten, dass diese in der Regel nicht objektivierbar ist, da subjektive Wahrnehmungen bzw. Präferenzen sowie situative Faktoren bzw. die Kontexte der Erstellung und Nutzung der Informationen die Beurteilung beeinflussen (Naumann, Rolker 2000, 148; Burgess et al. 2004, 375; Supekar et al. 2004, 2; Knight, Burn 2005, 162f).

Eppler (2003c) betrachtet die Informationsqualität im Kontext wissensintensiver Tätigkeiten und geht vom Grundproblem des Information Overload[184] aus, dessen zentrale Aussage darin besteht, dass rationale Entscheidungen oftmals durch ein Zuviel an Informationen behindert werden und somit Risikopotentiale in sich birgt. Von diesem Problem ausgehend liegt Informationsqualität dann vor, wenn Informationen die Eigenschaft aufweisen, Fragen in einer effizienten Art und Weise zu beantworten und Handlungen oder Entscheidungen zu ermöglichen (Eppler 2003a, 205). Analog zum Konzept Wissenstransfer geht die Nicht- bzw. Schlechterfüllung dieser Faktoren mit Risikopotentialen einher. Eppler sieht die Vernetzung von Informationsqualität und Wissensarbeit darin, dass Informationen

[183] Hinsichtlich des allgemeinen Qualitätsbegriffs identifiziert Garvin verschiedene Strömungen, die sich beispielsweise auf die Eigenschaften eines Produktes, die Zufriedenheit eines Nutzers, die Einhaltung von Anforderungen bei der Herstellung oder die Generierung eines Wertes beziehen (Garvin 1988, 40ff).

[184] Für weitere Details zum Information Overload siehe (Probst et al. 2000, 22).

einerseits einen Input für wissensintensive Tätigkeiten darstellen und zum anderen auch deren Ergebnis bzw. Output bilden und somit der Erhöhung ihres Wertes aus betriebswirtschaftlicher Sicht eine besondere Bedeutung zukommt (Eppler 2004, 323). Die Vernetzung zeigt sich weiter darin, dass Wissensarbeit durch eine Reihe von Risiken im Umgang mit Informationen gekennzeichnet ist. So können Informationen z.B. in ungeeigneter Menge vorliegen, ein unpassendes Format aufweisen oder bedingt durch eine starke Kontextualisierung nicht anwendbar sein (Eppler 2003c, 30ff). Aufgrund dieser Zusammenhänge werden die Aussagen zur Informationsqualität auch auf dokumentiertes Wissen angewandt, nachfolgend als Wissensqualität bezeichnet und folgendermaßen definiert.

Wissensqualität beschreibt die Eigenschaften wissensbezogener Ressourcen im Anwendungskontext und ergibt sich aus der Gesamtheit der Anforderungen, die sich auf die Eignung dieser Ressourcen zur Erfüllung gegebener Bedarfe bzw. Aufgabenstellungen beziehen.

Eine hohe Qualität der Informationen stellt potentiell einen Wettbewerbsvorteil dar, da aufgrund der Fülle der verfügbaren Informationen weniger der Zugang zu Informationen, sondern vielmehr deren Qualität ein Differenzierungskriterium darstellt (Bovee et al. 2003, 51; Beier 2005, 46). Die Sicherstellung der Informationsqualität erfordert eine grundlegende Analyse der Prozesse, Kompetenzen und der Erwartungen der Nutzer sowie zum Teil eine Veränderung von Arbeitsweisen und Prozessen (Eppler 2003c, 25).

Für die Beurteilung der Qualität dokumentierten Wissens können Kriterien verschiedener Dimensionen herangezogen werden. Dazu bestehen in der Literatur verschiedene Ansätze. So ziehen Königer und Reithmayer als Kategorien innere, kontextuelle, Zugangs- und Darstellungsqualität sowie die Qualität der Metainformationen und die Qualität der Strukturierung heran (Königer, Reithmayer 1998, 92). Naumann und Rolker setzen bei der Bildung von Qualitätskriterien am Nutzer, am Suchprozess und an der Informationsquelle selbst, also dem Inhalt, an und definieren dazu als korrespondierende Kategorien subjekt-, prozess- und objektbezogene Kriterien (Naumann, Rolker 2000, 152f). Zudem besteht eine Vielzahl an weiteren Frameworks zur Kategorisierung der Informationsqualität[185]. Eppler nimmt einen umfassenden Vergleich unterschiedlicher Kategorisierungsansätze vor und entwickelt ein Modell, mittels dessen die Qualität von Informationen und dokumentiertem Wissen in Bezug auf die Güte, die Community, in der die Erstellung und Anwendung erfolgt, die Prozesse zur Bereitstellung sowie die zugrunde liegende IT-Infrastruktur beurteilt werden kann. Weiterhin ordnet Eppler 16 Qualitätskriterien in diese vier Betrachtungsebenen und die Lebenszyklusphasen Identifikation, Bewertung, Aufbereitung und Anwendung ein (siehe Abb. 25), wobei deren Nicht- bzw. Schlechterfüllung das Niveau der Wissensqualität negativ beeinträchtigt und somit Risikopotentiale in sich birgt. Krite-

[185] Siehe hierzu z.B. (Kahn et al. 2002, 85f; Lee et al. 2002, 134f; Bovee et al. 2003, 55).

rien der Betrachtungsebenen Community und Güte können auch als Inhaltsqualität zusammengefasst werden, während Kriterien der beiden Ebenen Prozess und Infrastruktur zur Medienqualität subsumiert werden können (Eppler 2003c, 61, 68; 2004, 331). Die Lebenszyklusphase Identifikation umfasst beispielsweise das Auflisten möglicher Quellen, sowie das Finden der richtigen Quellen und der entsprechenden Informationen. Im Rahmen der Evaluierung werden z.B. die Glaubwürdigkeit, die Fehlerfreiheit und die Aktualität beurteilt sowie ein Vergleich mit anderen Quellen vorgenommen. Die Phase Aufbereitung schließt beispielsweise die Konvertierung des Formats, die Reduktion des Umfangs oder die Anreicherung des Inhalts ein, während die Lebenszyklusphase Anwendung die Informationen zur Problemlösung einsetzt und mit einer Routinisierung einhergehen kann (Eppler 2003c, 76f) [186].

Abb. 25 Ebenen der Informationsqualität [187]

Qualitätskriterien in der Betrachtungsebene Community zielen darauf ab, zu spezifizieren, inwiefern die Information die Bedürfnissen und Erwartungen der Nutzer der entsprechenden Zielgruppe erfüllen oder nicht. Dies betrifft im Detail die Fragestellungen, ob dokumentiertes Wissen komplett, genau, klar bzw. verständlich und anwendbar ist. Kriterien dieser Kategorie sind vom konkreten Verwendungskontext, in dem das dokumentierte Wissen eingesetzt wird, abhängig und im Vergleich zu den Kriterien der anderen Kategorien subjektiv. Die zweite Betrachtungsebene Güte wird durch die Kriterien kompakt, konsistent, korrekt und aktuell spezifiziert, wobei dokumentiertes Wissen kompakt ist,

[186] Das vollständige Modell von Eppler umfasst weitere Zusatzinformationen wie Managementprinzipien, Zielkonflikte zwischen den Kriterien oder die Zuweisung der Kriterien zu den Dimensionen Zeit, Kosten, Format und Inhalt. Demzufolge sind die Kriterien in Epplers Modell mehrfach kategorisiert. Im Kontext dieser Arbeit wurde eine Reduktion auf zwei Dimensionen vorgenommen, um die Komplexität zu senken und die für den Untersuchungsgegenstand relevanten Aspekte zu fokussieren.

[187] Abbildung nach (Eppler 2003c, 61, 68ff; 2004, 331).

wenn es frei von unnötigen Elementen ist sowie Konsistenz bei Freiheit von Widersprüchen und Korrektheit bei der Freiheit von Fehlern vorliegt. Aktualität als Anforderung trägt der geringen Halbwertszeit von Informationen und Wissen Rechnung. Die Qualität der Prozesse betrifft allgemein das Content Management und ergibt sich beispielsweise daraus, wie gut dokumentiertes Wissen bereitgestellt wird oder von den Nutzern nachgefragt werden kann. Die Qualität der Prozesse ist dann hoch, wenn dokumentiertes Wissen bequem, rechtzeitig, verantwortet und interaktiv nachgefragt werden kann. Während sich Bequemlichkeit darauf bezieht, inwiefern die Bereitstellung von dokumentiertem Wissen mit den Bedürfnissen und Gewohnheiten des Nutzers korrespondiert, bezeichnet das Kriterium rechtzeitig den Sachverhalt, dass die Information ohne Verzögerung von der Erstellung zur Nutzung bereitgestellt wird. Dokumentiertes Wissen ist dann verantwortbar, wenn überprüfbar ist woher es stammt und wer für die Erstellung verantwortlich ist. Das Kriterium interaktiv bezieht sich auf die Steuerbarkeit und die Anpassbarkeit der Prozesse. Die IT-Infrastruktur als vierte Betrachtungsebene soll sicherstellen, dass die Content Management Prozesse reibungslos ablaufen. Deren Qualität ist dann hoch, wenn die Inhalte zugänglich sind und sicher verwaltet werden. Darüber hinaus zeichnen die Wartbarkeit der Infrastruktur durch Administratoren und deren Schnelligkeit die Infrastruktur aus. Kriterien dieser Kategorie zeigen auf, dass die Informationsqualität nicht nur die Anforderungen der Nutzer zu berücksichtigen hat, sondern auch die Anforderungen derer, die mit der Verwaltung der Inhalte und Systeme betraut sind (Eppler 2003c, 67ff; 2004, 328ff).

In Bezug auf die Definition zu Wissensrisiko (siehe 5.1) sind Risiken auf die Nichterfüllung dieser Kriterien zurückzuführen. So kann beispielsweise in Bezug auf die Betrachtungsebene Community dokumentiertes Wissen durch andere Mitarbeiter nicht anwendbar sein und sich dies bei der Durchführung der Aufgaben in einem Mangel auswirken. Nicht fehlerfreie oder nicht aktuelle Inhalte können beispielsweise zu Fehlentscheidungen führen. Verzögerungen in Bezug auf die Bereitstellung der Inhalte von deren Erstellung zur Nutzung können sich ebenso wie eine mangelnde Nachvollziehbarkeit und mangelnde Nachvollziehbarkeit negativ auf die Wissensarbeit im Unternehmen auswirken und somit ein Risiko darstellen. Im Hinblick auf die IT-Infrastruktur können Wissensrisiken beispielsweise von einer mangelnden Zugänglichkeit bzw. Verfügbarkeit der Inhalte ausgehen. Zudem ist auch insbesondere die Sicherheit der verwalteten Inhalte von Bedeutung und kann in Verbindung mit der Wissensdiffusion den Wert der Inhalte reduzieren. Somit ist die Wissensqualität als breites Konzept auch im Zusammenspiel mit weiteren Risikoursachen zu beachten.

Wissensqualität kann neben der Nicht- bzw. Schlechterfüllung der in Abb. 25 dargestellten Kriterien auch dadurch negativ beeinträchtigt werden, dass Abhängigkeiten von wissensbezogenen Ressourcen bestehen und sich aus diesen Engpässen Mängel bei der Geschäftsprozessdurchführung ergeben. So kann beispielsweise der Ausfall von Mitarbeitern, die über knappe Kompetenzen verfügen, die Wissensqualität bedingt durch Nichtverfügbarkeit einschränken (van den Brink 2001, 42f; Kobi 2003,

13f). Neben internen Mitarbeitern können auch Abhängigkeiten vom Wissen von Kunden, Lieferanten und Partnern bestehen. So werden beispielsweise Produkte gemeinsam mit Lieferanten entwickelt oder das Feedback von Testkunden gezielt bei der Entwicklung bzw. Verbesserung der Produkte einbezogen, während in Kooperationsbeziehungen vielfach eine wechselseitige Spezialisierung erfolgt, die ebenfalls Abhängigkeiten und somit potentielle Engpässe schafft (Staudt 1992, 17). Im Hinblick auf in Objekten inkorporiertes Wissen können Abhängigkeiten von in IT-Systemen vorgehaltenem dokumentierten Wissen bestehen, wobei den IT-Systemen eine zunehmende Bedeutung für die Abwicklung der Geschäftsprozesse zukommt (Junginger, Krcmar 2003, 16f; Hirschmann, Romeike 2004, 13; Wolff 2005, 15).

5.6.2 Einzelrisiken

Personen: Risiken in Bezug auf die Kategorie Personen betreffen vorwiegend die Erstellung von Inhalten, also die konstruktive Wissensqualität (siehe auch 5.6.1). So können Wissensrisiken darauf zurückzuführen sein, dass Mitarbeiter Wissen für andere in einer ungeeigneten Art und Weise erstellen und somit die Anwendung dieses Wissens eingeschränkt bzw. verhindert wird. Zum anderen kann die Verfügbarkeit bzw. Zugänglichkeit des Wissens bedingt durch bestehende Abhängigkeiten eingeschränkt werden und in einem Mangel resultieren.

- **unzureichende Identifikation und Bewertung (QP1):** Insbesondere bei wissensintensiven Tätigkeiten ist es von Bedeutung, dass Mitarbeiter über Kompetenzen im Umgang mit Informationen und Wissen verfügen. Diese betreffen beispielsweise das Finden, Analysieren, Bewerten, Nutzen, Verdichten, Weitergeben und Generieren von Informationen. Insbesondere Methoden zur Filterung und eine kritische Reflexion der Qualität der Inhalte sind erforderlich[188], um aus der Fülle der verfügbaren die relevanten Informationen herauszufiltern und so dem Zustand des Information Overloads entgegenzuwirken (Kern et al. 1998, 14; Abell, Oxbow 2002, 128ff; Beier 2004, 133). Fehlen den Mitarbeitern diese Kompetenzen werden durch das Zuviel an Informationen Prozesse gehemmt. Weiterhin kann eine Folge der unzureichenden Identifikation und Bewertung von Inhalten zur Folge haben, dass Inhalte in die Wissensbasis integriert werden, die eine geringe Qualität aufweisen und auf dieser Basis Fehlentscheidungen getroffen werden.
- **unzureichende Erstellung und Weiterverarbeitung (QP2)**: Neben der unzureichenden Identifikation und Bewertung von Inhalten geht auch von deren unzureichender Erstellung und Weiterverarbeitung ein Wissensrisiko aus. So sollten Inhalte, die durch andere Mitarbeiter genutzt werden, bestimmte Qualitätsmerkmale erfüllen, um deren Anwendbarkeit zu gewährleisten. Daher sollten die Autoren bei der Erstellung darauf achten, dass die Inhalte vollständig, frei von Fehlern

[188] So kann eine geringe Qualität in diesem Zusammenhang beispielsweise darauf zurückgeführt werden, dass Inhalte aus Quellen mit einer geringen Verlässlichkeit genutzt werden (Kahn et al. 2002, 185, 187).

sowie inhaltlich korrekt sind. Ebenso ist bei der Erstellung darauf zu achten, dass auf subjektive Einstellungen verzichtet wird, da es so zu einer Verzerrung bzw. Fehlleitung kommen kann und dadurch die Bewertung durch andere unter Umständen erschwert wird (Strong et al. 1997, 40f). Darüber hinaus sollten die Inhalte für Dritte verständlich und auch relevant sein. Dies betrifft primär die Anpassung an die spezifischen Zielgruppen, die Adressaten darstellen. In Abhängigkeit ihrer Kenntnisse und Einbindung in die entsprechenden Prozesse sind weitere Kontextinformationen erforderlich, deren Fehlen die Einordnung und somit Verständlichkeit der Inhalte erschwert (Strong et al. 1997, 41; Bovee et al. 2003, 56). Ein Wissensrisiko im Bereich der Weiterverarbeitung ist auch darin zu sehen, dass bedingt durch das Kopieren, Bearbeiten und mehrfache Ablegen von Inhalten deren ursprüngliche Bedeutung verändert wird und die Veränderung nicht rekonstruierbar ist (Beier 2005, 46). Auf diese Weise kann die ursprüngliche Bedeutung verzerrt werden und eine fehlerhafte Interpretation der Inhalte zur Folge haben. Werden diese Qualitätskriterien (z.B. Klarheit, Vollständigkeit, Verständlichkeit) nicht erfüllt, kann die Anwendung der Inhalte durch andere Mitarbeiter erschwert werden (Eppler 2003a, 206f; Knight, Burn 2005, 162).

Insgesamt kann die Generierung fehlerhafter Inhalte und deren Weitergabe an in der Wertschöpfungskette nachgelagerte Mitarbeiter oder Partner zu Schäden im Allgemeinen und Fehlentscheidungen oder Zeitverzögerungen im Speziellen führen (Krcmar, Junginger 2003, 253).

- **Manipulation von Inhalten (QP4)**: Wissensrisiken im Hinblick auf eine eingeschränkte Qualität können sich daraus ergeben, dass Inhalte gezielt fehlerhaft erzeugt werden, so gesichert werden, dass sie für Dritte nicht auffindbar sind, deren Verbreitung unterdrückt wird oder bestehende Inhalte verändert werden. Eine derartige Manipulation kann zum Ziel haben, eine potentiell durch Dritte motivierte Fehlleitung zu erreichen oder eigene Interessen durchzusetzen (Alter 2006, 3). Das Schadensausmaß ist davon abhängig, inwieweit eine Manipulation gelingt und manipulierte Inhalte zur Anwendung gelangen.

Prozesse: Eine eingeschränkte Qualität kann dadurch hervorgerufen werden, dass die Prozesse in Bezug auf die Bereitstellung und Freigabe Schwächen aufweisen oder andere organisatorische Maßnahmen die Qualität negativ beeinträchtigen.

- **unbegleiteter unternehmensinterner Stellenwechsel (QO1)**: Während Inter- und Extrafluktuation (siehe 5.3.1) mit Wissensverlusten einhergehen, haben die Intrafluktuation bzw. unternehmensinterne Stellenwechsel eine Einschränkung der Qualität zur Folge, da das Wissen prinzipiell im Unternehmen vorhanden ist, aber die Zugänglichkeit erschwert sein kann (Williams 2004, 269ff). So wird durch unternehmensspezifische Karrierepfade oder Versetzungen die Zugänglichkeit zum Wissen der fluktuierten Mitarbeiter gehemmt, da die Wissensträger andere Stellen besetzen und dabei in anderen Abteilungen oder an anderen Standorten bzw. in anderen Regionen tätig

sind. Dabei schränkt zunehmende regionale Entfernung unter Umständen die Zugänglichkeit zu Wissen zusätzlich ein.

- **Mangel an qualifiziertem Personal (QO2)**: Das Vorhandensein qualifizierter Mitarbeiter ist erforderlich, um die entsprechenden Aufgaben im Rahmen der Erbringung der Wertschöpfung auszuführen. So sind im Speziellen Kompetenzen im Umgang mit Wissen (z.B. Identifizieren, Bewerten, Verarbeiten) oder IT-Systemen eine Voraussetzung dafür, dass die Mitarbeiter sicherheitsbewusst wissensintensive Tätigkeiten durchführen können (Abell, Oxbow 2002, 128ff; BSI 2006, 491). Das Fehlen bzw. die unzureichende Ausprägung dieser Kompetenzen kann darauf zurückgeführt werden, dass die Personalbeschaffung und Personalentwicklung ungeeignet im Sinne von lückenhaft erfolgen. In diesem Zusammenhang erschwert eine hohe Innovationsgeschwindigkeit das dauerhafte Erreichen bzw. Erhalten eines hohen Qualifizierungsgrades der Mitarbeiter (Harrant, Hemmrich 2004, 18)[189]. Der Erwartungswert in Bezug auf Engpässe und potentiell daraus resultierende Mängel nimmt zu, wenn Personal mit erforderlichen Kompetenzen nicht ausreichend beschafft wird, die Ausprägung der erforderlichen Kompetenzen nicht entsprechend überprüft wird oder eine unzureichende interne Entwicklung erfolgt (Kobi 1999, 13f; Knaese 2004, 45f). Darüber hinaus kann das Risiko zeitlich noch weiter vorgelagert sein und mit unzureichenden Personalbedarfsplanungen einhergehen[190].
- **mangelnde Verfügbarkeit von Kompetenzen (QO3)**: Neben dem Fehlen oder der unzureichenden Ausprägung von Kompetenzen können sich Risiken auch daraus ergeben, dass vorhandene Kompetenzen nicht ausreichend verbreitet sind und somit deren Verfügbarkeit begrenzt ist. Eine mangelnde Verbreitung kann zur Folge haben, dass aufgrund fehlender Redundanzen Engpässe bei der Geschäftsprozessdurchführung auftreten können. Neben unternehmensinternen Engpässen und somit der potentiellen Einschränkung der Zugänglichkeit können sich Wissensrisiken auch daraus ergeben, dass Abhängigkeiten von den Kompetenzen von Kooperationspartnern, Kunden, Lieferanten sowie externer Dienstleister bestehen (Schön 2004, 288)[191]. Derartige Abhängigkeiten bergen das Risiko in sich, dass sich die Engpässe in einem Mangel realisieren.

[189] Im Hinblick auf die Generierung der Wertschöpfung kann sich dies beispielsweise auf die Entscheidung über die Annahme von Aufträgen niederschlagen. So ist bei der Annahme von Mandanten oder Projekten zu prüfen, ob das Unternehmen mit vorhandenen Kompetenzen und Personalbestand in der Lage ist, die geforderte Gegenleistung zum erwarteten Zeitpunkt zu erbringen (Keßler, Winkelhofer 2002, 162; Pfitzer et al. 2002, 2007). Fehlen die entsprechenden Kompetenzen bzw. sind diese unzureichend, kann keine Annahme erfolgen, was in der Form eines entgangenen Gewinns zum Schaden des Unternehmens gereicht. Wird das Projekt oder der Mandant trotz negativer Prüfung angenommen kann dies aus einer allgemeinen Risikoperspektive zu einer Schlechtleistung und daraus resultierenden Reputationsverlusten führen.

[190] So kann beispielsweise eine fehlerhafte Bestimmung des qualitativen Personalbedarfs zur Folge haben, dass erforderliche Kompetenzen fehlen (Drumm 2000, 231ff).

[191] Abhängigkeiten können zudem die Verhandlungsmacht der Partner erhöhen, das Unternehmen erpressbar machen und die Wahrscheinlichkeit opportunistischen Verhaltens erhöhen (Schwamborn 1994, 241; de Laat 1999, 209).

- **unzureichende Gewährleistung der Aktualität (QO4)**: Aufgrund der kurzen Halbwertszeit bzw. der schnellen Innovationszyklen ist bestimmtes Wissen in der Wissensbasis des Unternehmens von einer Überalterung betroffen bzw. durch mangelnde Aktualität charakterisiert (z.B. Änderungen von Technologiestandards oder Gesetzestexten). Indikatoren für die Aktualität sind das Erstellungs- bzw. Überarbeitungsalter der Inhalte sowie die Volatilität des Themengebietes (Bovee et al. 2003, 56). So bestehen bestimmte Themen, die einer geringeren Veränderung unterliegen, während beispielsweise Erkenntnisse im Bereich neuer Technologien oder in der medizinischen Forschung hoch volatil sind. Die Anwendung nicht aktuellen Wissens kann zu Schäden führen, da potentiell Fehlentscheidungen getroffen werden und Reputationsverluste beim Kunden eintreten. Ein Risiko ergibt sich somit daraus, dass Aktualisierungsprozesse fehlen bzw. unzureichend sind und somit nicht aktuelles Wissen Anwendung findet (Amelingmeyer 2002, 156ff; Knaese 2004, 37; Desouza, Awazu 2005, 50).
- **unzureichende inhaltliche Überprüfung (QO5)**: Bevor Wissen zur Nutzung bereitgestellt wird, erfolgt eine Überprüfung der inhaltlichen Qualität im Hinblick auf Fehlerfreiheit, Vollständigkeit, inhaltliche Richtigkeit etc. Erfolgt dieser Prozess unzureichend, kann es zu einer Verbreitung von Wissenselementen geringer Qualität kommen und dies zu einem Mangel führen. Dieser Mangel kann sich dahingehend konkretisieren, dass Fehlentscheidungen getroffen werden (Eppler 2002, 1ff)[192].

Systeme: Risiken im Hinblick auf eine eingeschränkte Qualität können unter Bezugnahme auf das in Abschnitt 5.6.1 dargestellte Modell zur Beurteilung der Informationsqualität (siehe Abb. 25 auf Seite 180) neben subjektiven Kriterien der Nutzer auch auf die Infrastruktur bezogen sein, die eine entsprechende Bereitstellung zu gewährleisten hat. Diese Ebene des Modells korrespondiert mit der Ursachenkategorie Systeme.

- **unzureichende Verfügbarkeit von IT-Systemen (QS1)**: Ein Wissensrisiko bzgl. einer eingeschränkten Qualität kann sich auch daraus ergeben, dass Inhalte in IT-Systemen nicht zur Verfügung stehen und dadurch die Durchführung der Prozesse bzw. Aufgaben gehemmt wird. Dies kann durch Unzuverlässigkeiten bzw. Schwachstellen der technischen Infrastruktur verursacht werden, die beispielsweise das Resultat von Hard- und Softwaredefekten sein kann. Zudem können erfolgreiche Angriffe auf IT-Systeme, die durch eine unzureichende IT-Sicherheit ermöglicht wurden, eine Ursache der mangelnden Verfügbarkeit darstellen (Paulus 2000, 397; Peltier 2001, 13; Knaese 2004, 39). Die zunehmende Durchdringung der IT-Systeme und deren Schlüsselrolle bei der Durchführung von Prozessen unterstreicht die hohen Anforderungen an die Verfügbarkeit (Junginger, Krcmar 2003, 16f; Wolff 2005, 15). Engpässe in Bezug auf die Inhalte haben zur Fol-

[192] Für einen beispielhaften Genehmigungsprozess siehe (Bach et al. 2000, 76f).

ge, dass Redundanzen fehlen und somit der Ausfall eines IT-Systems bzw. dessen mangelnde Verfügbarkeit ein vergleichsweise höheres Schadensausmaß aufweisen kann.

- **zeitaufwändige Bereitstellung (QS2):** Neben der mangelnden Verfügbarkeit kann auch die Bereitstellung unzureichend sein und dadurch die Qualität eingeschränkt werden. Dies betrifft primär die für den Zugriff auf die Inhalte erforderliche Zeit. Diese kann beispielsweise durch eine umständliche oder nicht mit den Bedürfnissen und Gewohnheiten des Nutzers korrespondierende Navigation verursacht werden. Zudem können im Falle einer webbasierten Darstellung der Inhalte ein verwirrendes Layout, Inkonsistenzen oder zu viele Links und Hierarchiestufen zur Folge haben, dass der Zeitbedarf zur Bereitstellung bzw. Suche erhöht wird (Eppler, Muenzenmayer 2003, 187f). Ebenso erhöhen starke Sicherheits- und Geheimhaltungserfordernisse den erforderlichen Zeitbedarf. So kann beispielsweise eine mehrstufige Authentifizierung erforderlich sein, um die Inhalte nutzen zu können (Strong et al. 1997, 44; Bovee et al. 2003, 56).
- **unzureichend konsolidierte Quellen (QS3)**: Das Risiko einer eingeschränkten Qualität kann sich auch daraus ergeben, dass dieselben Inhalte zugleich in verschiedenen Quellen vorgehalten und Änderungen nicht konsolidiert werden. Dies hat zur Folge, dass Abweichungen bestehen und dies potentiell die Glaubwürdigkeit und Akzeptanz der Nutzer senkt (Strong et al. 1997, 40). Zudem kann auch die Aktualität der Inhalte negativ beeinträchtigt sein, falls diejenigen Quellen genutzt werden, auf die Aktualisierungen nicht übertragen wurden.
- **unzureichende Vertrauenswürdigkeit (QS4):** Ein weiteres Wissensrisiko besteht in einer unzureichenden Sicherheit der IT-Systeme, in denen Inhalte verwaltet werden, da dadurch die Vertrauenswürdigkeit reduziert wird. Dies betrifft vorwiegend das Verhalten in Bezug auf sensitive oder personenbezogene Inhalte (Eppler, Muenzenmayer 2003, 188; Rittberger 2004, 157, 162). Werden beispielsweise Kompetenzen der Mitarbeiter in Skillverzeichnissen, Ideen im betrieblichen Vorschlagswesen oder Dokumentationen zu Prototypen elektronisch verwaltet, so sind eine entsprechende Geheimhaltung und der Schutz vor unautorisierten Zugriffen erforderlich. Kann dies nicht gewährleistet werden oder sind bereits Sicherheitsvorfälle oder Missbrauch bekannt geworden, kann die Nutzung durch die Mitarbeiter negativ beeinträchtigt werden und somit erwartete Synergien ausbleiben.

externe Faktoren: Neben internen Ursachen der Kategorien Personen, Prozesse und Systeme kann eine eingeschränkte Qualität auch auf externe Faktoren zurückgeführt werden, wobei diese im Vergleich zu den beiden erstgenannten Risikokategorien Verlust und unerwünschte Diffusion von geringerer Relevanz ist, da Wissensqualität primär durch internes Handeln bzw. das Unterlassen von Handlungen beeinflusst wird.

- **unzureichende Inhaltsqualität der von Dritten bereitgestellten Inhalte (QE1)**: Wissensrisiken können sich daraus ergeben, dass Wissen, das im Rahmen von Kooperationen von den jeweiligen

Partnern empfangen wird, unternehmensinterne Qualitätskriterien nicht erfüllt. So kann z.B. mangelnde Fehlerfreiheit und Aktualität, hohe Subjektivität oder geringe Genauigkeit und Verständlichkeit vorliegen. Dies kann zur Folge haben, dass die Anwendung dieser Inhalte erschwert wird oder aufgrund einer zu ausgeprägten Subjektivität Fehlleitungen erfolgen. Dabei unterliegen externe Quellen vielfach auch einer hohen Veränderungsdynamik im Hinblick auf Inhalt und Qualität, die eine permanente Bewertung erforderlich macht (Naumann, Rolker 2000, 149, 156).

- **unzureichende Medienqualität der von Dritten bereitgestellten Inhalte (QE2)**: Werden Inhalte, die zur Durchführung bestimmter Aufgaben oder Prozesse erforderlich sind, außerhalb des Unternehmens bei Partnern oder Outsourcinganbieter vorgehalten, erwachsen daraus Risiken im Hinblick auf deren Verfügbarkeit und Bereitstellung. Eine unzureichende Gewährleistung der Medienqualität kann die Prozesse des Unternehmens hemmen (Nettesheim et al. 2003, 27; Rusch 2003, 13ff; BSI 2006, 427ff).
- **Manipulation der Inhalte durch Dritte (QE3)**: Neben der Manipulation durch interne Mitarbeiter können auch Dritte Inhalte manipulieren. Dies kann beispielsweise dadurch erfolgen, dass Dritte sich physischen Zugang verschaffen, extern in IT-Systeme eindringen oder im Zuge des Abhörens des Datenverkehrs Veränderungen an Nachrichten vornehmen (Alter 2006, 4ff; BSI 2006, 745).

5.6.3 Diskussion

Wissensqualität ist im Vergleich zu den zuvor betrachteten Konzepten primär unternehmensintern ausgerichtet und schließt vorwiegend Bewertungen der Mitarbeiter ein. Darüber hinaus unterliegt das Konzept wie in Abschnitt 5.6.1 dargelegt primär subjektiven Beurteilungen, wodurch die Risikobetrachtung erschwert wird. Wissensrisiken im Kontext der Wissensqualität treten in den vier Kategorien Personen, Prozesse, Systeme und externe Faktoren auf. Risiken in erstgenannter Kategorie betreffen mangelnde Kompetenzen im Umgang mit Informationen bzw. dokumentiertem Wissen und schließen Fehlhandlungen im Sinne einer gezielten Manipulation ein. Wissensrisiken, die der Kategorie Prozesse zuordenbar sind, betreffen die unzureichende Definition von organisatorischen Prozessen bzw. gehen von der Organisation zu verantwortenden Maßnahmen aus. In Bezug auf letztgenannte können interne Stellenwechsel unbegleitet sein sowie aufgrund unzureichender Personalbeschaffung oder auch -entwicklung Engpässe in Bezug auf das Personal bzw. spezifische Kompetenzen auftreten. Unzureichend definierte Prozesse können die mangelnde Gewährleistung der Aktualität der Inhalte sowie deren unzureichende inhaltliche Überprüfung betreffen. Wissensrisiken der Kategorie Systeme betreffen die zur Verwaltung und Bereitstellung des dokumentierten Wissens genutzten IT-Systeme. So können Risiken in diesem Zusammenhang Mängel in Bezug auf Verfügbarkeit, Bereitstellung, Konsolidierung der Quellen sowie Vertrauenswürdigkeit betreffen. Die Kategorie externe Faktoren schließt Wissensrisiken ein, die eine Manipulation oder unzureichende Bereitstellung von Inhalten durch Dritte betrifft.

Kategorie	No	Wissensrisiko
Personen	QP1	unzureichende Identifikation und Bewertung
	QP2	unzureichende Erstellung und Weiterverarbeitung
	QP3	Manipulation von Inhalten
Prozesse	QO1	unbegleiteter unternehmensinterner Stellenwechsel
	QO2	Mangel an qualifiziertem Personal
	QO3	mangelnde Verfügbarkeit von Kompetenzen
	QO4	unzureichende Gewährleistung der Aktualität
	QO5	unzureichende inhaltliche Überprüfung
Systeme	QS1	unzureichende Verfügbarkeit von IT-Systemen
	QS2	zeitaufwändige Bereitstellung
	QS3	unzureichend konsolidierte Quellen
	QS4	unzureichende Vertrauenswürdigkeit
externe Faktoren	QE1	unzureichende Inhaltsqualität der von Dritten bereitgestellten Inhalte
	QE2	unzureichende Medienqualität der von Dritten bereitgestellten Inhalte
	QE3	Manipulation der Inhalte durch Dritte

Tab. 11 Wissensrisiken der Kategorie Wissensqualität

Analog zu den zuvor behandelten Konzepten bestehen im Kontext der Wissensqualität Interaktionen, die aus der Literatur gestützt werden können. So kann eine unzureichende Erstellung oder Weiterverarbeitung von Inhalten durch die mangelnde Verfügbarkeit von Systemen oder eine zeitaufwändige Bereitstellung der Inhalte negativ beeinträchtigt werden, da so entweder zur Erstellung benötigte Inhalte nicht verfügbar sind oder diese aufgrund des zu hohen Zeitbedarfs vernachlässigt werden (Eppler 2003a, 207; Knaese 2004, 39). Derartige Hemmnisse können zur Folge haben, dass die Effizienz durch unverhältnismäßig hohen Zeitbedarf reduziert wird, die entsprechenden IT-Systeme nicht

genutzt werden und potentiell andere informelle Routinen zur Bereitstellung bzw. Nutzung entwickelt werden, die potentiell die Erreichung von Sicherheitszielen negativ beeinträchtigen[193]. Somit stehen Anforderungen an die Sicherheit in einem Trade-off mit einer schnellen Bereitstellung. Darüber hinaus können auch unzureichend konsolidierte Quellen die Erstellung bzw. Weiterverarbeitung der Inhalte negativ beeinträchtigen, da beispielsweise widersprüchliche Informationen vorliegen oder unterschiedliche Versionen bearbeitet werden (Strong et al. 1997, 40). Ebenso kann auch eine unzureichende Medienqualität Dritter im Sinne einer eingeschränkten Verfügbarkeit, zeitaufwändigen Bereitstellung oder eingeschränkten Vertrauenswürdigkeit die Erstellung bzw. Weiterverarbeitung von Inhalten negativ beeinträchtigen (Eppler 2003a, 207; BSI 2006, 643).

Weiterhin bestehen Austauschbeziehungen zwischen inhaltlicher Überprüfung, Aktualität und Bereitstellung. So zieht eine umfassende Überprüfung einen entsprechend hohen Zeitbedarf nach sich, wodurch die Aktualität gemindert wird. Eine Bereitstellung mit hohem Zeitaufwand kann dazu führen, dass Wissen bei Veröffentlichung und somit Nutzbarkeit bereits veraltet ist (Neus 2003, 44). Inhaltliche Freigabeprozesse, die mit einem hohen Zeitaufwand verbunden sind, reduzieren die Wahrscheinlichkeit, dass die Aktualität der bereitgestellten Inhalte hoch ist. Diese betrifft insbesondere Themengebiete mit einer hohen Volatilität.

Risiken im Bereich der Wissensqualität dürften auch eine starke Interaktion zu den Risiken anderer Konzepte aufweisen. So kann ein Mangel an verschiedenen Kompetenzen, der beispielsweise durch eine unzureichende Personalbeschaffung und -entwicklung verursacht wurde, Risiken im Bereich des Verlustes, der unerwünschten Diffusion und des unzureichenden Transfers hervorrufen. Somit kommt einer hohen Qualität in Bezug auf die Kompetenzen eine zentrale Bedeutung im Hinblick auf die anderen Risikokategorien zu. Auch Abhängigkeiten von Systemen oder den Kompetenzen einzelner Mitarbeiter können das Schadensausmaß von Risiken in Bezug auf den Wissensverlust erhöhen. Besteht beispielsweise eine Abhängigkeit von einem Mitarbeiter, der über Schlüsselkompetenzen verfügt und wird dieser Mitarbeiter abgeworben oder scheidet bedingt durch andere Faktoren aus dem Unternehmen aus, erhöht sich das Schadensausmaß des Wissensverlustes erheblich.

5.7 Ausgewählte konzeptübergreifende Interaktionen

Neben den konzeptinternen Interaktionen, die beispielhaft erörtert wurden, bestehen konzeptübergreifende Interaktionen. Diese werden aufgrund der hohen Anzahl an identifizierten Risiken, der daraus resultierenden Komplexität und der zum aktuellen Zeitpunkt nicht umfassenden Betrachtung des Untersuchungsgegenstandes in der Literatur und Praxis nachfolgend grob auf der Ebene der Konzepte betrachtet. Dabei sind einerseits Interaktionen zwischen den Konzepten Wissensverlust und Wissens-

[193] So können Mitarbeiter beispielsweise lokale Ablagestrukturen nutzen oder sensitive Inhalte über ungesicherte Kommunikationsverbindungen austauschen. Dies kann Wissensverluste oder eine unerwünschte Diffusion zur Folge haben.

diffusion von Relevanz, da die Risiken aufgrund der potentiellen externen Einflussfaktoren und der internen Anforderungen eng verwoben sind. Andererseits sind insbesondere auch Interaktionen zwischen den Konzepten Wissensdiffusion und Wissenstransfer bedeutend, da zwischen beiden Konzepten Austauschbeziehungen bestehen, die sich gegenseitig zumeist negativ bedingen. Diese Trade-offs werden auch in der Literatur zu interorganisationalen Arrangements wie strategischen Allianzen oder Joint Ventures vielfach thematisiert[194], da sich ein Dilemma aus dem Umfang und Nutzen des Wissenstransfers einerseits und dessen Begrenzung zur Reduktion einer unerwünschten Diffusion andererseits ergibt.

Interaktionen zwischen den Konzepten Wissensverlust und Wissensdiffusion: Fehlverhalten in Bezug auf Diffusion (DP1, DP2) und Verlust (VP4, VP5) betrifft jeweils unterschiedliche Aspekte, kann jedoch auch gleichlaufende Effekte haben bzw. Folgerisiken nach sich ziehen. So kann beispielsweise der Diebstahl eines Notebooks aufgrund mangelnder Sicherung einerseits Wissensverluste nach sich ziehen, andererseits aber auch Dritten ermöglichen, von sensitiven Inhalten Kenntnis zu nehmen, wodurch sich möglicherweise deren Exklusivität reduziert (Desouza, Vanapalli 2005, 86).

Risiken in Bezug auf die Zutritts- (VO6, DO1) und Zugriffsverletzungen (VO7, DO2) laufen ebenfalls in diesen beiden Konzepten gleich. So können Zutrittsverletzungen einen Diebstahl und somit einen Wissensverlust zur Folge haben und andererseits die bloße Kenntnisnahme ermöglichen und somit mit einer Wissensdiffusion einhergehen. Analoges gilt für Zugriffsverletzungen.

Auch in Bezug auf Angriffe auf IT-Systeme (VE4, DE9) verschwimmen zum Teil die Grenzen zwischen Risiken in Bezug auf die beiden Konzepte, weshalb eine strikte Trennung schwer möglich ist. So kann beispielsweise eine Aushorchung von Mitarbeitern bzw. Social Engineering dazu genutzt werden, Zugriff auf IT-Systeme zu erhalten. Als Konsequenz können, wie bereits erwähnt, sowohl Verluste durch Löschung oder Manipulation als auch eine Diffusion erfolgen. Analoges gilt für das Einschleusen von Schadsoftware, wie z.B. Trojanische Pferde, die dazu genutzt werden können, Zugangsdaten oder sensitive Inhalte auszuspionieren oder diese im Falle eines erfolgreich ausspionierten Zugangs zu löschen (BSI 2006, 691f). Ebenso kann technisches Versagen (VS1, DS2) beide Konzepte betreffen.

Interaktionen zwischen den Konzepten Wissensdiffusion und Wissenstransfer: Im Hinblick auf die Konzepte Wissenstransfer und -diffusion bestehen gegenläufige Beziehungen, da die Zielsetzungen konträr sind. Ein Zielkonflikt besteht im Hinblick auf die Intensität der Zusammenarbeit (TO4, DO4). So kann umfassende Kontrolle der Zusammenarbeit durch den Einsatz von Gatekeepern oder Genehmigungsprozessen zwar Risikopotentiale im Hinblick auf die unerwünschte Diffusion, wie z.B. opportunistisches Verhalten, reduzieren, allerdings auch eine Hemmung der Wissenstransferprozesse

[194] Siehe z.B. (Hamel et al. 1989, 136; Sanchez 1995, 3; Baughn et al. 1997, 104; Appleyard, Kalsow 1999, 288; Kale et al. 2000, 217; Mitchell et al. 2002, 3; Mohr, Sengupta 2002, 282; Norrman, Lindroth 2004, 610; Oxley, Sampson 2004, 723).

und somit eine Reduktion der Potentiale und des Erfolgs des Wissenstransfers haben (Hamel et al. 1989, 134ff; Lei 1993, 40; Oxley, Sampson 2004, 727). Weiterhin können Sicherheitsrichtlinien, die zur Unterdrückung der Diffusion eingesetzt werden, aber auch die Wahrscheinlichkeit erhöhen, dass der Partner die Anforderungen bzw. Maßnahmen als Misstrauen interpretiert, folglich dessen Leistungsbereitschaft abnimmt und somit die erwünschten Wissenstransferprozesse gehemmt werden (Norman 2004, 613). Darüber hinaus können rigide Sicherheitsrichtlinien in Bezug auf die Mitarbeiter zur Folge haben, dass bedingt durch zeitaufwendige Sicherheitsmaßnahmen oder Genehmigungsprozesse die Mitarbeiter ihre Aktivitäten im Hinblick auf den Wissenstransfer mit Partnern reduzieren (Barth 2001, 4). Bedingt durch potentielle Gegenreaktionen der Partner, die in Bezug auf die Ausgewogenheit der Kooperationsbeiträge mit einer Leistungsreduktion einhergehen können, kann so der Wissenstransfererfolg negativ beeinträchtigt werden.

Ein analoges Problem ergibt sich daraus, dass einerseits dem Partner Vertrauen entgegengebracht werden muss, um die Wissenstransferprozesse zu unterstützen. Andererseits kann dieses Vertrauen Raum für opportunistisches Verhalten bieten und durch den Partner zum Nachteil des Unternehmens ausgenutzt werden. Da sich Risiken im Hinblick auf beide Konzepte ergeben können, ist ein geeignetes Maß an Kontrolle zu finden. Die Erörterung dieser Fragen ist Gegenstand der Handlungsempfehlungen (siehe Kapitel 8), die auf den Erkenntnissen aus der Literatur und der empirischen Studie aufbauen.

5.8 Zusammenfassung und Diskussion

In den vorangegangenen Abschnitten wurden die Einzelrisiken zu den vier Teilkonzepten, die sich aus der Definition zu Wissensrisiken ableiten lassen, erläutert. Wissensrisiken in Bezug auf das Konzept Wissensverlust betreffen primär personengebundenes und in Objekten inkorporiertes Wissen, während organisatorisch verankertes Wissen von Wissensverlusten eher gering betroffen ist, es sei denn es ergeben sich Kumulationen. In Bezug auf dieses Konzept stehen Risiken vielfach im Kontext der Fluktuation, die verschiedene unternehmensinterne und -externe Ursachen aufweisen kann. Angriffe auf IT-Systeme können als permanente Bedrohung gesehen werden, die vergleichsweise stark interagiert und eine Reihe personeller, organisatorischer oder technischer Schwachstellen nutzen kann. Das Schadensausmaß in Bezug auf den Verlust dokumentierten Wissens wird darüber hinaus durch die Wiederherstellbarkeit beeinflusst, die sich daraus ergibt, inwiefern Wissen durch Personen rekonstruiert werden kann.

Wissensrisiken im Kontext der Wissensdiffusion sind dadurch gekennzeichnet, dass viele interne und externe Akteure aktiv oder passiv an der Diffusion beteiligt sein können und dadurch der Variantenreichtum dieser Risiken zunimmt. Zudem sind diese Risiken primär außenorientiert, da sie mit einer Reduktion der Exklusivität und somit des Wertes der wissensbezogenen Ressourcen einhergehen kön-

nen. Aus diesem Grund sind vergleichsweise viele Wissensrisiken der Wissensdiffusion der Kategorie externe Faktoren zuordenbar.

Bedingt durch eine Fokussierung des Wissenstransfers auf Sender, Empfänger und entsprechende Rahmenbedingungen sind im Vergleich zu den anderen Konzepten weniger Akteure involviert. Da Risiken dieses Konzeptes zu den Diffusionsrisiken gegenläufig sind, ist bei einem zielorientierten und integrierten Umgang mit Wissensrisiken diese Austauschbeziehung zu beachten, da eine Übersteuerung im Bereich der Wissensdiffusion die erwünschten Prozesse im Kontext des Wissenstransfers hemmen kann.

Auch die Risiken im Kontext der Wissensqualität sind durch eine vergleichsweise geringere Anzahl an involvierten Akteuren charakterisiert und primär unternehmensintern ausgerichtet. Bezugnehmend auf die relevanten Dimensionen der Wissensqualität bestehen Austauschbeziehungen zwischen den Kriterien. So steht beispielsweise die Gewährleistung der Aktualität im Konflikt mit einer zeitnahen Bereitstellung der Inhalte. Analoges gilt in Bezug auf die Infrastruktur im Hinblick auf die Verfügbarkeit und die Sicherheit des Systems, die mit dessen Vertrauenswürdigkeit in Zusammenhang steht.

Weiterhin sind die Risiken in Bezug auf diese Konzepte nicht isoliert voneinander zu betrachten, sondern interagieren untereinander. Einige auf der Literatur basierende konzeptinterne Interaktionen wurden in den vorangegangenen Abschnitten beispielhaft erwähnt. Es ist davon auszugehen, dass bei einer systematischen und langfristigen Auseinandersetzung mit Wissensrisiken in der Praxis und der Forschung umfassende Interaktionen identifiziert werden, wie dies auch bei Risikogruppen der Fall ist, die seit langem in Unternehmen gesteuert werden (z.B. finanzwirtschaftliche Risiken). Zum aktuellen Stand der Forschung ist jedoch keine tiefgehende fundierte Betrachtung der Interaktionen möglich. In nachfolgenden Abschnitten werden der Prozess zum Management von Wissensrisiken sowie konkrete Steuerungsmaßnahmen erörtert.

5.9 Kernaufgaben des Wissensrisikomanagements

In folgenden Abschnitten wird das Management von Wissensrisiken erörtert, wobei eine Anlehnung an den traditionellen RM-Prozess (siehe Abschnitt 3.5) sowie die Besonderheiten des IT-RM erfolgt (siehe Abschnitt 4.3). Letzteres hebt sich insbesondere dahingehend vom traditionellen RM ab, als dass vielfach eine ressourcenfokussierte Sichtweise eingenommen wird. Ein derartiger Fokus erscheint auch für das Management von Wissensrisiken aufgrund der zentralen Rolle wissensbezogener Ressourcen besonders geeignet.

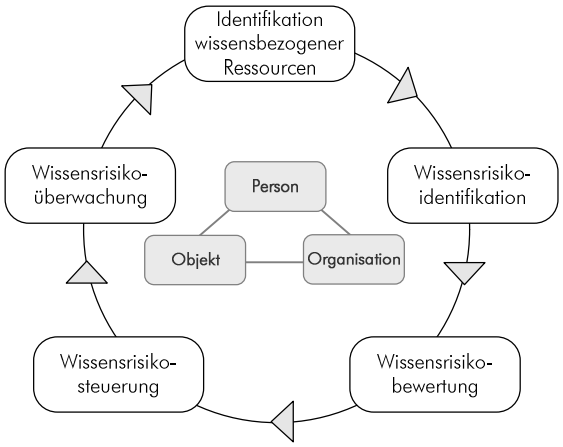


Abb. 26 Wissensrisikomanagementprozess

Die Wissensbewertung spiegelt in diesem Kontext eine Integration der Bewertung von Risiken allgemein und der Wertbestimmung von Wissen (siehe Abschnitt 2.3) wider. Auch Gaudig (2005, 5f) lehnt den Wissensrisikomanagementprozess an den betriebswirtschaftlichen RM-Prozess an und sieht den Zusammenhang in der Erweiterung des Repertoires der Steuerungsmaßnahmen um Maßnahmen und Instrumente des WM. Basierend auf den Erläuterungen zum RM und IT-RM umfasst der Wissensrisikomanagementprozess fünf Prozessphasen (siehe Abb. 26), die in den nachfolgenden Abschnitten erläutert werden. Die Schnittstelle von RM und WM zeigt sich insbesondere darin, dass den traditionellen Phasen des RM eine Identifikation von wissensbezogenen Ressourcen vorgelagert wird und eine Voraussetzung für nachgelagerte Prozessphasen darstellt. Weiterhin fließen Maßnahmen des WM in den Katalog potentieller Steuerungsmaßnahmen ein.

5.9.1 Identifikation wissensbezogener Ressourcen

Wie in Abschnitt 5.2 dargestellt, beziehen sich die Ursachen von Wissensrisiken auf wissensbezogene Ressourcen. Diese Sichtweise liegt auch mehreren Ansätzen im IT-RM (siehe Abschnitt 4.3) zugrunde. In diesem Kontext ist es bedeutend, den Schutzbedarf der IT-Ressourcen zu bestimmen und entsprechend der Schutzwürdigkeit die Risiken zu managen. Eine analoge Ausrichtung erscheint auch für das Management von Wissensrisiken zweckdienlich, wobei ein effizientes und zielgerichtetes Vorgehen voraussetzt, dass Transparenz über die vorhandenen und eingesetzten wissensbezogenen Ressourcen besteht. Demzufolge muss klar sein, welche wissensbezogenen Ressourcen im Unternehmen vorhanden sind und welchen Wert sie aufweisen.

Eine derartige Transparenz ist dann gegeben, wenn in Unternehmen gezielt Maßnahmen eingesetzt werden, die diese fördern. So ergibt sich eine Erhöhung der Transparenz z.B. daraus, dass im Unternehmen Bestrebungen zum Management des intellektuellen Kapitals bestehen. Diese haben zum Ziel, sowohl unternehmensintern als auch -extern aufzuzeigen, welche intellektuellen Potentiale im Unternehmen vorhanden sind und wie diese zukünftig ausgeschöpft bzw. erhöht werden können. Dies setzt eine detaillierte Identifikation und Wertbeimessung voraus, der Gegenstand von Abschnitt 2.3 ist. Im unternehmensinternen Fall besteht ein Ziel darin, Werttreiber zu identifizieren und durch deren gezieltes Management eine Performanceverbesserung zu erreichen (Marr et al. 2004, 553).

Weiterhin wird im Rahmen des Personalmanagements und im Speziellen der Personalentwicklung versucht, durch die Erstellung und laufende Aktualisierung von Kompetenzprofilen die Transparenz über das vorhandene Mitarbeiterwissen zu erhöhen. Ein gezielter Einsatz von Kompetenzprofilen oder Skillverzeichnissen dient beispielsweise der Identifikation von Experten, Personalentwicklung oder Unterstützung des Projektmanagements durch systematische Besetzung von Projektteams (Gebert, Kutsch 2003, 237f; Gronau, Uslar 2004, 135f). Jedoch wird ein umfassender Teil der Mitarbeiterkompetenzen aus Datenschutzgründen oder aufgrund anderer Ursachen nicht erfasst, wodurch die potentielle Transparenz eingeschränkt wird (Probst et al. 2006, 67).

Nicht zuletzt ist die Schaffung von Transparenz auch ein Ziel des WM. Durch die systematische Identifikation und Aufbereitung von Themen sowie der entsprechenden Wissensträger, die im Wesentlichen die Typen wissensbezogener Ressourcen (siehe Abschnitt 2.2.3) widerspiegeln, kann diese ebenso erhöht werden. Der Nutzen der Transparenz ist darin zu sehen, dass sich die Orientierung in Bezug auf das im Umfeld verfügbare Wissen verbessert und somit durch eine effiziente Nutzung wissensbezogener Ressourcen die Handlungsfähigkeit des Unternehmens erhöht wird (Probst et al. 2006, 64f). Zur Erhöhung der Transparenz können verschiedene Instrumente des WM herangezogen werden. So können die Skillverzeichnisse, die eine Schnittstelle zum Personalmanagement darstellen, um verschiedene Wissenskarten, die Quellen, Strukturen, Träger und Anwendungen von Wissen zueinander in Beziehung setzen, die Erhöhung der Transparenz unterstützen (Eppler 2003b, 189ff; Probst et al. 2006, 67ff).

Amelingmeyer sieht in der Transparenz und Erreichbarkeit der Wissensträger eine Voraussetzung für die Nutzung von Wissen. So können Stellenbeschreibungen und Organigramme zu einer verbesserten Transparenz beitragen. Dies trifft auch auf einheitliche und intuitive Ablagesysteme zu. Darüber hinaus können spezifische Rollen wie Wissensbroker die Transparenz erhöhen und somit die Identifikation wissensbezogener Ressourcen erleichtern. Zusätzlich kann auch eine systematische papierbasierte oder elektronische Verbreitung dokumentierten Wissens die Transparenz verbessern (Amelingmeyer 2002, 141ff)

Knaese und Probst heben im Gesamtprozess des RM der Mitarbeiterfluktuation diesen Schritt hervor. Demnach sollten im Rahmen eines effizienten Managements zuerst die zentralen Wissensträger identifiziert werden, deren Fluktuation dem Unternehmen zu einem besonderen Schaden gereichen würde. In Bezug auf die weiteren Phasen des Prozesses erfolgt in einem zweiten Schritt eine Bewertung der Wahrscheinlichkeiten, dass diese Mitarbeiter das Unternehmen verlassen, während in einem dritten Schritt Steuerungsmaßnahmen im Hinblick auf die Mitarbeiterbindung determiniert werden (Knaese, Probst 2001, 36).

Somit kann sich die Identifikation der vorhandenen wissensbezogenen Ressourcen auf verschiedene Quellen stützen. Neben der bloßen Identifikation ist es allerdings auch von Bedeutung, dass seitens

der Unternehmung definiert wird, welche wissensbezogenen Ressourcen eine besondere Werthaltigkeit aufweisen. Zu diesem Zweck kann eine Klassifikation von Wissen herangezogen werden, die sich auf verschiedene Faktoren stützt. So kann zur Klassifikation zum einen die Vertraulichkeit der wissensbezogenen Ressourcen herangezogen werden. Diese ist umso höher, umso mehr die wissensbezogenen Ressourcen die Kernkompetenzen des Unternehmens tangieren bzw. zur Wertgenerierung beitragen. Die Klassifikation kann sich auch am potentiellen Schadensausmaß orientieren, das entstehen würde, wenn nicht autorisierte Dritte Kenntnis von den sensitiven Inhalten nehmen (Dreger 1998, 361). Im Hinblick auf eine Operationalisierung der Klassifikation kann die Werthaltigkeit in Abhängigkeit der Vertraulichkeit, des Wertschöpfungsbeitrags, der Wettbewerbsrelevanz oder des potentiellen Schadensausmaßes bei Kenntnisnahme durch unautorisierte Dritte auf der Ebene von Themen bestimmt werden. Diese Vorgabe kann Top Down hoch aggregiert erfolgen und den Themen verschiedene Klassifikationsstufen wie streng geheim, geheim, vertraulich oder nur für Dienstgebrauch zuweisen (McGonagle, Vella 1994, 295; Lux, Peske 2002, 164)[195]. Auf den darunter liegenden Hierarchieebenen, wie z.B. Geschäftsbereichen und Abteilungen, können diese groben Vorgaben operationalisiert und ergänzt werden.

So kann eine Klassifikation auf der Ebene der operativen Geschäftsprozesse zur Folge haben, dass Maßnahmen zur Steuerung, wie z.B. Geheimhaltungspflichten für spezifisches dokumentiertes Wissen, bestehen. Neben der Klassifikation der Inhalte kann auch eine Klassifikation des Status von Personen bestimmt werden. Demzufolge ist die Zuordnung zu einer bestimmten Sicherheitsstufe eine Voraussetzung dafür, dass Personen auf klassifiziertes Wissen zugreifen können. Dabei kann die Klassifikation von Inhalten einerseits und der Vergabe eines Status an Personen andererseits mit Problemen behaftet sein, da bei ungeeigneter Definition vielfach Anpassungen vorgenommen werden, die die Kategorisierung beispielsweise durch das Erhöhen des Status unterlaufen (Nosek 2006). Daher muss einerseits die Definition der Klassifikationen wohl durchdacht sein und andererseits darf eine Änderung der Stufen nicht den Regelfall darstellen (Dreger 1998, 361). Zudem ist in diesem Kontext zu beachten, dass eine extensive Klassifikation bzw. eine Überklassifikation, erwünschte Prozesse, wie z.B. Transferprozesse, hemmen kann, da zusätzliche Maßnahmen durch die Mitarbeiter ergriffen werden müssen, die einen entsprechenden Zeitaufwand nach sich ziehen (Desouza, Vanapalli 2005, 87f).

Insgesamt ist eine grobe Klassifikation wissensbezogener Ressourcen erforderlich, um eine effiziente Steuerung von Wissensrisiken in Bezug auf alle vier Konzepte zu erzielen. So kann eine Klassifikation im Hinblick auf die Konzepte Wissensverlust und Wissensdiffusion dazu beitragen, dass werthaltige wissensbezogene Ressourcen vergleichsweise mehr Schutz und demzufolge rigidere Maßnahmen

[195] Eine detaillierte Betrachtung wie eine derartige Klassifikation erfolgen kann ist Gegenstand des Abschnittes 8.1 im Kapitel Handlungsempfehlungen.

erfahren. Zum anderen schafft eine derartige Klassifikation auch Transparenz darüber, welches Wissen im Rahmen von Kooperationen transferiert werden kann oder nicht (Norman 2001, 52ff). In Bezug auf das Konzept Wissensqualität können auf der Basis einer derartigen Klassifikation mit zunehmender Werthaltigkeit vergleichsweise höhere Qualitätsanforderungen definiert werden. Somit nimmt die Klassifikation von Wissen auch auf diese beiden Konzepte Einfluss bzw. stellt ebenfalls eine Voraussetzung dar.

Da Unternehmen über eine Vielzahl an wissensbezogenen Ressourcen verfügen und eine vollständige Steuerung aller wissensbezogenen Ressourcen weder möglich noch ökonomisch wäre, kann die durch die Identifikation geschaffene Transparenz herangezogen werden, um festzulegen, welche wissensbezogenen Ressourcen in die Steuerung einbezogen werden sollen und somit ein Beitrag zum gezielten Ressourceneinsatz und einer systematischen Steuerung geleistet werden (Verfassungsschutz 2004b, 8).

5.9.2 Wissensrisikoidentifikation

Wie in Abschnitt 3.5.2 dargestellt, können verschiedene Ausgangspunkte für die Identifikation von Risiken herangezogen werden. So können einerseits Geschäftsprozesse und dabei insbesondere diejenigen, die zur Erbringung der Wertschöpfung einen kritischen Beitrag leisten, eine geeignete Ausgangsbasis bilden. Zudem kann die Risikoidentifikation über einzelne Geschäftsbereiche hinweg durchgeführt werden. Zur Unterstützung der Identifikation können in diesen Fällen bestehende Kategorisierungen zu Risiken herangezogen werden, um ein strukturiertes Vorgehen sicherzustellen. Die Relevanz der jeweiligen Risiken ist dabei je nachdem welche Geschäftsbereiche oder Prozesse analysiert werden unterschiedlich, da die Aufgaben und die Einbeziehung externer Akteure variiert. Für die Identifikation von Wissensrisiken trifft ein analoges Vorgehen zu, wobei der größte Unterschied zur klassischen Risikoidentifikation darin zu sehen ist, dass eine Unterstützung durch Risikokategorisierungen aufgrund des Neuheitsgrades dieser Thematik bisweilen nicht systematisch erfolgt. Im Bereich des traditionellen RM haben sich mittlerweile Standards herausgebildet, nach denen Risiken kategorisiert werden[196]. Zudem bestehen in Unternehmen langjährige Erfahrungen zum RM, die mitunter auf gesetzliche Verpflichtungen (z.B. KonTraG) zurückzuführen sind und eine Adaptierung dieser Standards auf die unternehmensspezifischen Besonderheiten zur Folge haben. Darüber hinaus haben sich auch unternehmensindividuell geeignete Lösungen entwickelt. Analog verhält es sich im Bereich des IT-RM. Auch hier bestehen zahlreiche Standards, die die Identifikation von Risiken erleichtern[197]. So können z.B. die IT-Grundschutzkataloge und im Speziellen die Gefährdungskataloge herangezogen werden, um Risiken systematisch zu identifizieren (BSI 2006). Ebenso bestehen im Bereich des Ma-

[196] Siehe z.B. (Diederichs et al. 2004, 190) und Abschnitt 3.4.
[197] Siehe hierzu Abschnitt 4.4.

nagements operationeller Risiken ähnliche Bestrebungen[198]. Im Rahmen dieses Abschnittes soll daher analog eine Kategorisierung entwickelt werden, die eine systematische Identifikation von Wissensrisiken über Geschäftsprozesse oder Geschäftsbereiche hinweg unterstützt. Der Vorschlag zur Kategorisierung von Wissensrisiken basiert auf den in den Abschnitten 5.3-5.6 erörterten Wissensrisiken.

	Verlustrisiken	Diffusionsrisiken	Transferrisiken	Qualiätsrisiken
Personenrisiken	• unbegleiteter Ruhestand (VP1) • Beendigung der Erwerbstätigkeit (VP2) • Unternehmenswechsel (VP3) • fahrlässiges Fehlverhalten (VP4) • vorsätzliches Fehlverhalten (VP5) • mang. IT-Kompetenz (VP6)	• fahrlässiges Fehlverhalten (DP1) • vorsätzliches Fehlverhalten (DP2)	• Zurückhaltung aufgrund Unsicherheit (TP1) • mangelndes Vertrauen (TP2) • Abwehr- / Vermeidungshaltung (TP3) • unzureichende Explizierung (TP4) • unzureichende Absorbierung (TP5)	• unzureichende Identifikation und Bewertung (QP1) • unzureichende Erstellung und Weiterverarbeitung (QP2) • Manipulation von Inhalten (QP4) • mangelnde Anwendbarkeit (QP5)
Prozessrisiken	• Reorganisationsverlust (VO1) • Nichtdokumentation (VO2) • Nachfolgeverlust (VO3) • Vertretungsverlust (VO4) • Übergabeverluste(VO5) • Zutrittsverletzung (VO6) • Zugriffsverletzung (VO7) • unbegleitete Beendigung der Zusammenarbeit (VO8)	• Zutrittsverletzung (DO1) • Zugriffsverletzung (DO2) • unkontrollierter Einsatz temporär beschäftigter Mitarbeiter (DO3) • unkontrollierte interorganisatorische Zusammenarbeit (DO4) • unkontrollierte Veröffentlichung (DO5)	• unbegleitete Reorganisation (TO1) • unbegleitete Beendigung von Projekten (TO2) • fehlende Transparenz über vorhandenes Wissen (TO3) • eingeschränkte Zusammenarbeit (TO4) • hemmende Sicherheitsrichtlinien (TO5) • Inkompatibilität zwischen den Partnern (TO6)	• unbegleiteter unternehmensinterner Stellenwechsel (QO1) • Mangel an qualifiziertem Personal (QO2) • mangelnde Verfügbarkeit von Kompetenzen (QO3) • unzureichende Gewährleistung der Aktualität (QO4) • unzureichende inhaltliche Überprüfung (QO5)
Systemrisiken	• technisches Versagen / Fehlfunktionen (VS1) • mangelnde Wiederherstellbarkeit (VS2)	• mangelnde Sicherung der IT-Systeme (DS1) • technisches Versagen / Fehlfunktionen (DS2)	• Bereitstellung unzureichender Medien (TS1) • unzureichende Anwenderfreundlichkeit (TS2) • unzureichende Vertrauenswürdigkeit (TS3)	• unzureichende Verfügbarkeit von IT-Systemen (QS1) • zeitaufwändige Bereitstellung (QS2) • unzureichend konsolidierte Quellen (QS3) • unzureichende Vertrauens-würdigkeit (QS4)
Risiken aus externen Ereignissen	• Abwerbung (VE1) • Personalausfall (VE2) • Diebstahl (VE3) • Angriff auf IT-Systeme (VE4) • höhere Gewalt (VE5)	• Aushorchung (DE1) • Einschleusung (DE2) • Anwerbung (DE3) • opportunistisches Verhalten der Partner (DE4) • unzureichende Vertraulichkeitswahrung durch Partner (DE5) • Reverse Engineering (DE6) • Diebstahl (DE7) • Abhören (DE8) • Angriff auf IT-Systeme (DE9) • Sicherheitsverstoß durch Partnern (DE10) • Anwendung von Wissen durch ehemalige Mitarbeiter (DE11)	• mangelnde Leistungsfähigkeit des Partners (TE1) • mangelnde Leistungsbereitschaft des Partners (TE2) • Schutzverhalten des Partners (TE3)	• unzureichende Inhaltsqualität der von Dritten bereitgestellten Inhalte (QE1) • unzureichende Medienqualität der von Dritten bereitgestellten Inhalte (QE2) • Manipulation der Inhalte durch Dritte (QE3)

Tab. 12 Kategorisierung von Wissensrisiken

Diese Kategorisierung basiert somit auf der Literaturanalyse und bedarf einer weiteren Verfeinerung im Praxiseinsatz. Sie schließt dabei sowohl die vier generischen Ursachen operationeller Risiken als auch die spezifischen Ursachen von Wissensrisiken ein. Um die Relevanz der in Tab. 12 kategorisierten Wissensrisiken zu überprüfen, können im Rahmen der Risikoidentifikation entlang der Geschäftsbereiche oder -prozesse verschiedenste Quellen herangezogen werden. Dabei kann die Identifikation von Wissensrisiken generell durch die klassischen Instrumente und Methoden, wie z.B. Workshops, standardisierte Interviews, Checklisten, Prozess- oder Fehlerbaumanalysen, unterstützt werden[199]. Im Speziellen können Verträge mit Mitarbeitern oder externen Partnern im Hinblick auf bestehende Verpflichtungen zur Geheimhaltung geprüft werden. Im Falle von Outsourcingabkommen kann sich eine

[198] Siehe z.B. (Doering 2001, 20; van den Brink 2001, 4ff; Piaz 2002, 57; Simon 2002, 130ff; Jorion 2003, 538; KPMG 2003, 3).

[199] Für die verschiedenen Methoden der Risikoidentifikation und entsprechende Quellen siehe Abschnitt 3.5.2.

derartige Prüfung auch auf Verpflichtungen zur Erbringung der Serviceleistungen sowie auf Fragen der Haftung beziehen. Die Identifikation von Risikopotentialen in Bezug auf die Sicherheit der IT-Systeme kann beispielsweise die Durchführung von Penetrationstests, Überprüfung der Leistungsfähigkeit der Datensicherung, Auswertung von Protokollierung im Hinblick auf unautorisierte Zugriffe etc. einschließen. Weiterhin können in Bezug auf die Identifikation von Wissensrisiken im Bereich der Wissensqualität beispielsweise Kompetenzprofile aus der Personalabteilung herangezogen werden, um potentielle Engpässe an Kompetenzen zu identifizieren. Betrachtet man die Wissensrisikoidentifikation anhand des Risikos einer Zugriffsverletzung (DO2), so können als potentielle Quellen, die die Identifikation stützen Logdateien, Meldungen der Mitarbeiter oder Überprüfungen der Aktualität der Zugriffsrechte herangezogen werden.
Wie auch bei der klassischen Risikoidentifikation ist die Definition eines Abbruchkriteriums, auf Basis dessen der betriebene Aufwand mit den Auswirkungen potentiell unentdeckter Risiken abgewogen wird (Faisst, Kovacs 2002, 11), aus ökonomischer Sicht erforderlich, da insbesondere bei Wissensrisiken aufgrund der angeführten Probleme der Erfolg der Identifikation vergleichsweise geringer einzuschätzen ist. Wie auch im Falle operationeller Risiken (Jovic, Piaz 2001, 924) ist bedingt durch die Neuheit des Themengebiets und das mangelnde Bewusstsein für Wissensrisiken eine vollständige Identifikation dieser Risiken unwahrscheinlich.

5.9.3 Wissensrisikobewertung

Wissensrisiken sind wie auch operationelle Risiken (siehe Abschnitt 3.3) aufgrund ihrer Natur schwierig zu quantifizieren, da insbesondere dynamische Umfeldbedingungen die Eintrittswahrscheinlichkeit und das Schadensausmaß dieser Risiken beeinflussen (Füser et al. 2002, 498; Locher et al. 2004, 22).
Die Bewertbarkeit unterscheidet sich je Einzelrisiko. Im Falle von klassischen Risiken, wie z.B. Kredit- und Marktrisiken, die bereits über viele Jahre hinweg bewertet werden, kann auf historische Risikodatenbanken zurückgegriffen werden und so beispielsweise die Ausfallwahrscheinlichkeit von Krediten oder im Falle von Rückversicherern die Wahrscheinlichkeit von Risiken höherer Gewalt durch langjährige Dokumentation hinreichend gut prognostiziert werden. Im Falle von Wissensrisiken liegen derartige historische Risikoeintrittswahrscheinlichkeiten oder Schadensausmaße aufgrund der Neuigkeit des Themengebietes nicht vor. Während im Bereich des operationellen RM im Bankensektor eine systematische Sammlung und Aufbereitung erfolgt, fehlt eine derartige Systematik im Bereich Wissensrisikobewertung zum aktuellen Zeitpunkt gänzlich. Dennoch sind in Unternehmen Daten vorhanden, die zur Ermittlung des Risikoerwartungswertes herangezogen werden können. Insbesondere für Risiken, die den Konzepten Wissensverlust und Wissensdiffusion zugeordnet sind, können verschiedene Quellen herangezogen werden. Zieht man das zuvor angeführte Beispiel zur Zugriffsverletzung (DO2) erneut heran, so sind zur Ermittlung des Erwartungswertes die Bewertung der Eintrittswahr-

scheinlichkeit und des Schadensausmaßes erforderlich. Erstere kann sich auf historische Daten der Zugriffsverletzungen bzw. die Zahl des Auftretens in einem bestimmten Zeitraum beziehen. Analoges gilt für das Schadensausmaß, zu dessen Bestimmung historische Schadensdaten herangezogen werden können, wobei zusätzlich der Wert der betroffenen Ressourcen einbezogen werden sollte. So kann sich das Schadensausmaß z.B. an historischen Schadensersatzforderungen orientieren, die auf eine vorangegangene Zugriffsverletzung zurückgehen.

Dazu werden nachfolgend beispielhafte Quellen zu Eintrittswahrscheinlichkeiten für Risiken der Kategorien Personen, Prozesse, Systeme und externe Ereignisse erläutert. Potentielle Quellen stellen dabei Statistiken des Unternehmens, Auswertungen der IT-Abteilung sowie die Einschätzung der Mitarbeiter dar. Eine vollständige Auflistung potentieller Quellen zur Bewertung der Einzelrisiken, die erste Anhaltspunkte geben soll, ist Gegenstand des Anhangs (siehe Anhang A3 auf Seite 446ff).

- **Personenrisiken**: Für die Ermittlung der Eintrittswahrscheinlichkeit der Fluktuation können Berufsunfähigkeitsquoten, die jährliche allgemeine Fluktuation oder die Fluktuation zu Konkurrenten im Speziellen herangezogen werden. Ebenso kann die Anzahl der in den nächsten Jahren altersbedingt ausscheidenden Mitarbeiter vergleichsweise sicher prognostiziert werden. Zudem werden in der Praxis Befragungen eingesetzt, mittels derer die Arbeitsplatzzufriedenheit der Mitarbeiter evaluiert wird, um so die Fluktuationsneigung in Erfahrung zu bringen (Klingler et al. 2004, 3f). Bedeutend schwerer fällt hingegen die Ermittlung von Eintrittswahrscheinlichkeiten im Hinblick auf das Fehlverhalten von Mitarbeitern. In diesem Kontext wird im Bereich des operationellen RM im Bankenbereich versucht, historische Daten zu sammeln und auf der Basis Eintrittswahrscheinlichkeiten zu prognostizieren (Stickelmann 2002, 10). Derartige Risikodatenbanken können auch für das Management von Wissensrisiken herangezogen oder aufgebaut werden. Darüber hinaus kann die Einschätzung durch Führungskräfte die Risikobewertung unterstützen. Ebenso wie Fehlverhalten kann sich die Ermittlung eines Mangels an Kompetenzen an Risikodatenbanken operationeller Risiken orientieren bzw. die Einschätzung durch Führungskräfte bzw. Personalverantwortliche nutzen.
- **Prozessrisiken**: Zur Bewertung von Prozessrisiken kann im Hinblick auf die Definition von Zutritts- und Zugriffsrechten ebenso wie bzgl. der Implementierung von Sicherheitsrichtlinien eine Orientierung an bestehenden Standards erfolgen und das Risikopotential auf der Basis von Abweichungen ermittelt werden[200]. Zur Einschätzung von Risiken in Bezug auf Nachfolge, Reorganisation, Vertretung, Übergabe sowie unkontrollierte Zusammenarbeit kann eine Bewertung durch die jeweils risikoverantwortlichen Mitarbeiter erfolgen. Dies gilt im Besonderen auch für die Bewertung von Prozessrisiken im Bereich des Wissenstransfers und der Wissensqualität.

[200] Siehe hierzu z.B. (Verfassungsschutz 2004b; BSI 2006).

- **Systemrisiken**: Bezüglich IT bezogener Risiken können verschiedene externe Statistiken z.B. zur Häufigkeit und zum Schaden von Angriffen, zur Verlust- und Diebstahlsquote von mobilen Endgeräten o.ä. herangezogen werden. Darüber hinaus können unternehmensintern auch Logfiles, Systemausfallzeiten, Dokumentationen zu Sicherheitsfällen etc. Quellen für die Risikobewertung bilden[201]. Zudem können in diesem Bereich auch Standards, wie z.B. die IT-Grundschutzkataloge, herangezogen werden, um bestehende Sicherheitsmaßnahmen abzugleichen und daraus Risikopotentiale abzuleiten. Ebenso können Wahrscheinlichkeiten in Bezug auf technisches Versagen oder erfolgreiche Angriffe auf der Basis unternehmensinterner historischer Daten oder unter Zugrundelegung externer Studien in diesem Themengebiet prognostiziert werden. Insbesondere in Bezug auf Systemrisiken, die dem Konzept Wissenstransfer zugeordnet sind, sollte eine Risikoeinschätzung durch die Mitarbeiter erfolgen.
- **Risiken aus externen Ereignissen**: Zur Ermittlung der fluktuationsbezogenen Risiken aus externen Ereignissen können Absentismus- und Krankheitsquoten ebenso wie Abwerbeversuche durch Konkurrenten herangezogen werden. Risiken der Anwerbung, Einschleusung und Aushorchung sind ebenso wie Abhörversuche, opportunistisches Verhalten oder eingeschränkte Leistungsbereitschaft schwer prognostizierbar, da sie verdeckt erfolgen. Daher sollten zur Risikobewertung historische Erwartungswerte hochgerechnet werden und um Einschätzungen durch operative Risikoverantwortliche ergänzt werden. Für Diebstähle oder Angriffe auf IT-Systeme können die analogen Quellen wie bei den Systemrisiken genutzt werden. Speziell die Risiken des Reverse Engineering sollten durch Mitarbeiter eingeschätzt werden, die tiefgehend Kenntnisse zu den Produkten des Unternehmens haben, und diese Einschätzung um historische Fälle ergänzt werden.

Neben der Ermittlung der Eintrittswahrscheinlichkeiten ist eine Bestimmung des Schadensausmaßes für die Bildung eines Risikoerwartungswertes erforderlich. Als Basis können die Ansätze zur Bewertung immaterieller Ressourcen (siehe Abschnitt 2.3) sowie Indikatoren im Rahmen der freiwilligen Berichterstattung (siehe Abschnitt 2.3.4) einen Beitrag leisten. Im IT-RM, das ebenfalls von Bewertungsproblemen im Hinblick auf die betroffenen Ressourcen gekennzeichnet ist, basiert die Wertbestimmung auf mehreren Faktoren. So werden einerseits die Beschaffungs- oder Wiederherstellungskosten der Ressourcen herangezogen, andererseits werden auch potentiell mögliche Schäden, die sich aus der Verletzung der IT-Schutzziele[202] ergeben, in die Wertermittlung einbezogen. Zu diesen zählen beispielsweise Schäden aus der Verletzung gesetzlicher Vorschriften, Umsatzeinbußen oder Reputationsverluste (Queensland 2001, 22f; Yapp 2003, 173f).

Ein Kernproblem besteht allerdings darin, dass die den wissensbezogenen Ressourcen inhärente Dynamik die Bewertung erschwert. Auch im Falle einer unerwünschten Diffusion ist der Wert der wis-

[201] Siehe hierzu z.B. (DTI 2004; Ernst&Young 2004; CSI/FBI 2005; Vile 2007).
[202] Siehe hierzu Abschnitt 4.2.

sensbezogenen Ressourcen heranzuziehen, da dieser durch den Verlust der Exklusivität verloren gehen kann. Problematisch ist dabei insbesondere die Tatsache, dass das Schadensausmaß durch das Ausmaß des Verlustes an Exklusivität bestimmt wird. Demzufolge kann sich im Falle der Diffusion die Ermittlung am Schaden orientieren, der entstehen würde, wenn nicht autorisierte Dritte Kenntnis von den sensitiven Inhalten nehmen (Dreger 1998, 361). Dabei wird das Schadensausmaß auch dadurch beeinflusst, inwiefern Dritte das diffundierte Wissen erfolgreich rekontextualisieren und somit auch gewinnbringend einsetzen können. Auf den gewinnbringenden Einsatz nehmen insbesondere die Eigenschaften der wissensbezogenen Ressourcen z.B. im Hinblick auf Komplexität und Spezifität (siehe Abschnitt 2.2.4) ebenso wie die Fähigkeiten des Dritten Einfluss. Da der Erfolg auch von den Fähigkeiten Dritter beeinflusst wird, fällt die Prognose des Schadensausmaßes schwer bzw. ist nicht in reliabler Form möglich.

Ebenso wie im klassischen RM ist auch die Beachtung von Interaktionen zwischen den Einzelrisiken erforderlich, um kompensatorische und kumulative Effekte zu berücksichtigen. Erste grobe Anhaltspunkte für potentielle Interaktionen wurden in den Abschnitten 5.3-5.7 gegeben. Diese Interaktionen sind allerdings nur ein erster Indikator, welche Risiken bei Annahme gleicher Erwartungswerte aufgrund ihres hohen Interaktionsgrades primär gesteuert werden sollten. Jedoch besteht aufgrund der Neuheit des Themengebiets noch umfassender Forschungsbedarf sowohl im Hinblick auf die relevanten Wissensrisiken als auch in Bezug auf die Interaktionen zwischen diesen. Die Wissensrisikobewertung schließt mit der Aggregation der Einzelrisiken unter Beachtung der Interaktionen ab[203].

Wie auch die Bewertung operationeller Risiken (Jovic, Piaz 2001, 924) hängt eine quantitative Bewertung der Wissensrisiken vom Umfang und Qualität der verfügbaren Daten ab und wird davon limitiert. Da diese vielfach nicht vorliegen, muss auf qualitative Bewertungsverfahren zurückgegriffen werden. Insgesamt ist eine quantitative auf historischen Daten basierende Risikoeinschätzung zu präferieren[204]. Da das Management von Wissensrisiken und somit die Beachtung dieser Risikokategorie vergleichsweise gering ist, empfiehlt es sich wie im Falle operationeller Risiken entsprechende Risikodatenbanken aufzubauen. Dies ist vergleichsweise gut möglich im Bereich der Fluktuation, da in diesem Fall verschiedene Personalstatistiken genutzt werden können. Auch im Falle von IT bezogenen Risiken können Logfiles oder ähnliche Dokumentationen herangezogen werden. Sofern möglich sollte die Bewertung durch Eintrittswahrscheinlichkeiten aus externen Studien gestützt werden. Dies ist v.a. im Kontext der IT-Sicherheit möglich. Speziell zur Beurteilung der Risiken in Bezug auf die beiden Konzepte Wissenstransfer und Wissensqualität kann vielfach nur die Einschätzung durch die Mitarbeiter

[203] Erste Erkenntnisse zur Relevanz von Wissensrisiken wurden in der empirischen Studie gewonnen, die Gegenstand der Kapitel 6 und 7 ist.

[204] Deren Einsatz wird allerdings dadurch erschwert, dass die Risikoursachen sehr unterschiedlich und idiosynkratisch sind, da dies die Verlässlichkeit der Daten negativ beeinträchtigt (Williams et al. 2006, 73).

erfolgen, wobei im Falle erstgenannter Kategorie Kooperationsverantwortliche einbezogen werden sollten.

5.9.4 Wissensrisikosteuerung

Die Steuerung von Wissensrisiken orientiert sich an der klassischen Risikosteuerung, nach der die Alternativen Vermeidung, Verminderung, Überwälzung, Akzeptanz und Teilung von Risiken zur Verfügung stehen, wobei letztgenannte eine Handlungsalternative im interorganisatorischen Fall darstellt. Die Handlungsalternativen korrespondieren im Wesentlichen mit dem traditionellen RM[205], während Unterschiede primär die Alternative Überwälzen betreffen. Aufgrund des Neuheitsgrades des Themenfeldes und der daraus resultierenden geringen Verbreitung in der Praxis bestehen zum aktuellen Zeitpunkt nur wenige Versicherungslösungen. In Bezug auf operationelle Risiken kann man diese Risikogruppe als Gesamtpaket versichern und somit Betrugsfälle und IT-Risiken einschließen. Auch in Bezug auf IT-Risiken, wie z.B. Ausfall von Systemen, bestehen Versicherungslösungen (Gordon et al. 2003, 82)[206].

Jedoch sind bedingt durch Komplexität und Volatilität des Themengebietes Versicherungslösungen in Bezug auf IT-Risiken von einigen Schwierigkeiten gekennzeichnet. So wird die Preisbestimmung dadurch erschwert, dass keine Vergangenheitsdaten vorhanden sind und zudem Sicherheitsvorfälle bzw. -schäden oftmals von Unternehmen nicht veröffentlicht werden, da befürchtet wird, dass dies negative Auswirkungen auf z.B. Reputation oder Aktienkurs haben könnte. Die Preisbestimmung wird zudem durch schwer prognostizierbare Interaktionen erschwert. Während physische Schäden meist geographisch begrenzt sind, können sich Schäden in vernetzten Systemen innerhalb kurzer Zeit weltweit verbreiten (z.B. Schadsoftware). Zudem sind Versicherungslösungen allgemein auch durch die adverse Selektion und das moralische Risiko charakterisiert. Zur Reduktion beider Problematiken fordern Versicherungsgeber zum Teil Security Audits oder Zertifizierungen und gewähren Rabatte, wenn Sicherheitsmaßnahmen implementiert sind (Gordon et al. 2003, 82f; Müßig 2006, 41). Im Zusammenhang mit der Nichtverfügbarkeit von Wissensträgern bieten einige Versicherer eine Schlüsselpersonenversicherung an, die bei Unfall, Krankheit und Tod von Mitarbeitern eintritt. Durch diese Art von Versicherung werden die für die Beschäftigung von Aushilfen, die Einarbeitung von neuen Mitarbeitern oder die Zusatzkosten für Auftragsvergabe außer Haus entstandenen Aufwendungen und zum Teil sogar der Abbruch von Geschäftsverbindungen gedeckt (Kiechle 2001, 19).

Die Informationsbasis für die Steuerung von Wissensrisiken ist im Vergleich zu klassischen Risiken wie Markt- oder Kreditrisiken geringer, da die Bewertung von Wissensrisiken (siehe Abschnitt 5.9.3) noch in den Anfängen steht und insbesondere durch die mangelnde Transparenz über wissensbezoge-

[205] Siehe hierzu auch Abschnitt 3.5.4.
[206] Zur Versicherbarkeit von IT-Risiken gibt (Koch 2005) einen guten Überblick.

ne Ressourcen sowie deren Dynamik erschwert wird. Dadurch wird auch ein gezieltes Ergreifen von Steuerungsmaßnahmen erschwert. Das IT-RM ist dadurch gekennzeichnet, dass eine Vielzahl an möglichen Risiken besteht, die von verschiedensten Akteuren ausgehen können, und somit eine hohe Komplexität vorliegt, die eine detaillierte Betrachtung der Risiken erschwert bzw. verhindert. Zudem ist eine reaktive Steuerung bestimmter Risiken, wie z.B. der Verlust an Integrität oder Vertraulichkeit von sensitiven Inhalten, nicht zielführend, da diese dann bereits nicht mehr nutzbar sind oder an Wert eingebüßt haben. Diese Probleme werden in den entsprechenden Ansätzen und Standards dadurch behoben, dass ein Set an Steuerungsmaßnahmen präventiv und somit losgelöst von der Risikobewertung ergriffen wird (siehe z.B. IT-Grundschutzkataloge in Abschnitt 4.4.2), um so einen Schutz vor potentiell eintretenden Risiken zu erreichen. Ein derartiges Vorgehen eignet sich auch für die Steuerung von Wissensrisiken, da auch hier umfassende Bewertungsprobleme bestehen und dadurch die für eine klassische Steuerung erforderliche Informationsbasis unzureichend ist. Somit kann durch ein präventiv orientiertes Vorgehen eine Kompensation der Bewertungsprobleme erreicht werden. Auf der anderen Seite geht ein derartiges Vorgehen mit anderen Problemen einher, die primär die Rechtfertigung der Aufwendungen für die Steuerungs- bzw. Sicherungsmaßnahmen betreffen. So ist wie im Falle des IT-RM nur schwer der Nachweis zu erbringen, dass Ersparnisse bzw. die Verhinderung von Schäden auf die ergriffenen Maßnahmen zurückzuführen sind, da der Eintritt der Risikoereignisse unsicher ist (siehe Abschnitt 4.3). Insbesondere das Ausbleiben von Schäden z.B. in Bezug auf die Verhinderung von Interfluktuation dürfte nur schwer quantifizier- bzw. vermittelbar sein. Speziell auch im Bereich der Steuerung von Wissensrisiken, die bedingt durch den Personenbezug von Wissen eine Unterstützung durch die Mitarbeiter erfordert, entstehen Kosten daraus, dass die Einhaltung der entsprechenden Regelungen und Richtlinien kontrolliert wird (Liebeskind 1997, 636).

Rekurriert man wiederum auf das konkrete Beispiel einer Zugriffsverletzung (DO2), so können zur Steuerung dieses Risikos einerseits die Zugriffsrechte adaptiert werden und andererseits die entsprechenden organisatorischen Richtlinien, die Fehlverhalten in Bezug auf Zugriffsverletzungen sanktionieren, angepasst werden. Weiterhin können zur Abwehr externer Zugriffsverletzungen Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen werden.

Bei der Steuerung von Wissensrisiken und der Ermöglichung von Prozessen des WM besteht generell ein Dilemma, das aus der erforderlichen Abwägung zwischen Freigebigkeit und Sicherheit resultiert (Lee, Rosenbaum 2003; Upadhyaya et al. 2006, 795; Wilson et al. 2006, 787). Die erwünschten Prozesse des WM, wie z.B. unternehmensinterne und -übergreifende Transferprozesse oder die Erhöhung der Transparenz über im Unternehmen vorhandenes Wissen, können durch eine zu umfassende Steuerung, die auch als Übersteuerung bezeichnet werden kann, negativ beeinträchtigt werden. Zudem kann eine zu starke Betonung der Schutzmaßnahmen im Speziellen zu einem Missverhältnis zwischen Arbeitnehmer und Arbeitgeber führen und dabei insbesondere durch das erzeugte Misstrauen das Be-

triebsklima negativ beeinträchtigt werden. Zudem können Wissenstransferprozesse bzw. Kommunikationswege gestört werden und dies negative Auswirkungen auf die organisatorische Effizienz haben (Maier 1992, 102; Liebeskind 1997, 637f). Dabei kann es auch der Fall sein, dass Mitarbeiter Maßnahmen, die als die Arbeitsprozesse hemmend empfunden werden, umgehen. Aus diesen Gründen setzt eine effiziente Steuerung von Wissensrisiken einen entsprechenden Verhaltenswandel der Mitarbeiter und deren Überzeugung voraus (Barth 2001, 4).
Eine ausführliche Betrachtung des Konzeptes Steuerung und entsprechender Maßnahmen ebenso wie eine Erstellung von Beziehung zu den in den Abschnitten 5.3-5.6 behandelten Wissensrisiken erfolgt in Abschnitt 5.10.

5.9.5 Wissensrisikoüberwachung

Ebenso wie im klassischen RM hat die Überwachung im Bereich des Managements von Wissensrisiken eine Überprüfung der risikopolitischen Entscheidungen auf ihre Wirksamkeit und ihren ökonomischen Nutzen zum Gegenstand. Dies bedeutet im Detail die Überprüfung der Effizienz der Identifikations-, Bewertungs- und Steuerungsmaßnahmen bzw. -instrumente, die eine Anpassung zur Folge haben kann. Im konkreten Fall betrifft dies eine Erweiterung und Adaption des in Abschnitt 5.9.2 dargelegten Katalogs an Wissensrisiken. Zum Zweiten sind auch im Bereich der Risikobewertung sowohl im Hinblick auf die Einschätzung der Eintrittswahrscheinlichkeiten als auch bei der Bestimmung des Schadensausmaßes Anpassungen zu erwarten, wenn ein Einsatz in Unternehmen erfolgt und die erste Bewertung reflektiert wird. So können sich alternative Quellen als geeigneter herausstellen. Analoges gilt für die Wirksamkeit der Steuerungsmaßnahmen. Deren Effizienz kann auf der Basis von sieben Anforderungen, die durch Hillson definiert wurden, ermittelt werden (Hillson 1999, 2). Bei den Anforderungen handelt es sich im Einzelnen um die nachfolgend beschriebenen Aspekte. (1) Appropriate: So müssen diese angemessen im Hinblick auf den Risikoerwartungswert sein. (2) Affordable: Zum Zweiten müssen die Steuerungsmaßnahmen eine gewisse Effizienz in Bezug auf das Kosten-Nutzen Verhältnis aufweisen und zudem sollte ein entsprechendes Budget je Steuerungsmaßnahme definiert sein. (3) Actionable: Des Weiteren ist ein Zeitfenster zu definieren, in dem die Bewältigung des Risikos zu erfolgen hat. Dabei ziehen einige Risiken sofortigen Handlungsbedarf nach sich, während andere zu einem späteren zeitlichen Horizont bewältigt werden können. (4) Achievable: Als weitere Anforderung muss eine Maßnahme sowohl aus technischer Hinsicht oder in Bezug auf die erforderlichen Fähigkeiten leistbar sein. (5) Assessed: Im Sinne des RM-Prozesses ist nach Durchführung einer Maßnahme eine Rückkopplung und somit eine Bewertung ihrer Wirkung erforderlich, um die Effizienz einer zukünftigen Anwendung zu verbessern. (6) Agreed: Darüber hinaus stellt Konsens zwischen den Stakeholdern über den Einsatz der Steuerungsmaßnahmen eine weitere Anforderung dar, die insbesondere auch im Falle unternehmensübergreifender Risiken von Relevanz ist. (7) Allocated

and Accepted: Letztlich sollte die Verantwortung für eine Maßnahme einer Person zugewiesen werden, der somit auch deren Durchführung zugerechnet werden kann. Nachdem die Phasen des RM-Prozesses durchlaufen wurden, können auch Risikoindikatoren definiert werden und auf deren Basis Prozesse überwacht werden.
Zieht man das Beispiel des Managements des Risikos einer Zugriffsverletzung (DO2) erneut heran, so könnte im Rahmen der Wissensrisikoüberwachung laufend die Aktualität der Zugriffsrechte geprüft werden. Zudem sollte geprüft werden, inwiefern sich Zugriffsverletzungen seit der Steuerung reduziert haben oder nicht, um die Effizienz der Steuerungsmaßnahmen bewerten zu können.

5.10 Steuerung von Wissensrisiken

Die Steuerung von Wissensrisiken stellt neben den zuvor in den Abschnitten 5.3-5.6 dargestellten Konzepten den Hauptuntersuchungsgegenstand dieser Arbeit dar, der auch Bestandteil der empirischen Studie ist (siehe Kapitel 6 und 7). In diesem Abschnitt wird ein Klassifikationsschema zur Einordnung der Steuerungsmaßnahmen entwickelt und darauf basierend Maßnahmen, die den entsprechenden Kategorien zugeordnet werden können, vorgestellt. Abschließend werden die Steuerungsmaßnahmen den diskutierten Wissensrisiken zugeordnet und deren Einfluss erörtert. Dabei soll ebenso wie bei den Interaktionen aufgezeigt werden, welche Maßnahmen sich im Besonderen eignen, einen Großteil der Risiken zu steuern. Eine derartige Konzentration ist auch in ökonomischer Hinsicht von Bedeutung, da Wissensrisiken ebenso wie auch Risiken im Bereich der Wirtschaftskriminalität durch vielfältige Ursachen ausgelöst werden können und somit ein vollkommener Schutz nicht möglich ist (Verfassungsschutz 2004b, 8). Daher stellen Empfehlungen zur gezielten Allokation von Steuerungsmaßnahmen ein wichtiges Teilergebnis dieses Abschnittes dar.

5.10.1 Klassifikation von Steuerungsmaßnahmen

Die Steuerung von Wissensrisiken stellt zum aktuellen Zeitpunkt kein etabliertes Konzept dar. Es können jedoch Anleihen aus verschiedenen Wissenschaftsdisziplinen genommen werden, die speziell auf die in den Abschnitten 5.3-5.6 erörterten Wissensrisiken adaptiert werden können. Zum einen können Maßnahmen aus dem IT-RM entliehen werden, da in diesem Kontext IT-Ressourcen und im Speziellen Informationen, die es zu schützen gilt, vordergründig betrachtet werden. Der Schutzbedarf ergibt sich dabei aus der Werthaltigkeit dieser Ressourcen und kann durch die Definition von IT-Schutzzielen (siehe Abschnitt 4.2) konkretisiert werden. Dabei korrespondiert das Schutzziel Vertraulichkeit mit der Wissensrisikoursache unerwünschte Diffusion, da in beiden Fällen das Risiko und der damit einhergehende Schaden durch den Verlust an Exklusivität verursacht werden. Die Schutzziele Integrität und Verfügbarkeit stehen in Zusammenhang mit der Wissensrisikoursache eingeschränkte Qualität, da auch sie mit einer unzureichenden Erfüllung von Qualitätskriterien im Zusammenhang

mit den Medien bzw. Inhalten (siehe Abschnitt 5.6) stehen. Auch die Authentifikation und das höhere Ziel Zugriffskontrolle können auf die Wissensrisikoursachen Verlust und Diffusion gleichermaßen übertragen werden, da diese Ziele gewährleisten sollen, dass nur autorisierte Personen auf die Inhalte zugreifen können. Schmidt unterscheidet in diesem Kontext zwischen organisatorischen, technischen und rechtlichen Maßnahmen zur Gewährleistung der IT-Sicherheit, während Hansen und Neumann rechtliche Maßnahmen unter die organisatorischen subsumieren und als dritte Kategorie physikalische Maßnahmen anführen, die bauliche Aspekte betreffen (Hansen, Neumann 2005, 285; Schmidt 2006, 97).

Zum Zweiten ergeben sich Anknüpfungspunkte in Bezug auf Steuerungsmaßnahmen auch aus Ansätzen, die auf die Abwehr von Wirtschaftsspionage bzw. Competitive Intelligence Bestrebungen anderer Unternehmen abzielen (Maier 1992; McGonagle, Vella 1994; Dreger 1998; Lux, Peske 2002; Verfassungsschutz 2004b; Erickson, Rothberg 2005; Meissinger 2006). Diese Maßnahmen verfolgen primär das Ziel zu verhindern, dass sensitive Inhalte in den Erkenntnisbereich von Dritten und im Speziellen von Konkurrenten gelangen und so an Wert einbüßen. Somit stehen diese Maßnahmen primär im Zusammenhang mit der Steuerung einer unerwünschten Diffusion. Zudem ist auch die Wissensrisikoursache Verlust betroffen, da systematisch durch Zugangskontrollen und weitere Absicherungen Einbrüche und Diebstähle verhindert werden sollen. Maier bringt die Maßnahmen mit den für ihn zentralen Risiken Einschleusung, Abwanderung, Anwerbung und Abschöpfung in Zusammenhang (Maier 1992, 99). Diese Risiken sind auch Gegenstand der in Abschnitt 5.4 dargelegten Risiken, die im Kontext der Wissensdiffusion stehen. Allgemein weisen Maßnahmen zur Abwehr von Competitive Intelligence bzw. Wirtschaftsspionage einen personellen, organisatorischen, baulichen / technischen oder juristischen Fokus auf (Dreger 1998, 299; Lux, Peske 2002, 173ff; Verfassungsschutz 2004b, 9).

Aus diesen Ansätzen lassen sich Kategorisierungen für Steuerungsmaßnahmen ableiten. So können einerseits organisatorische Steuerungsmaßnahmen als Kategorie angeführt werden, die nach dieser Sichtweise auch Maßnahmen in Bezug auf Personen einschließen. Sie betreffen somit primär Maßnahmen in Bezug auf die Vergütung, Führung, Richtlinien etc. Als zweite Kategorie können technische Maßnahmen angeführt werden, die beispielsweise die Sicherung der Integrität und Vertraulichkeit von in IT-Systemen verwalteten Inhalten einschließen. Diese Maßnahmen stehen auch in Zusammenhang mit den organisatorischen Maßnahmen, da sie diese vielfach umsetzen. So werden beispielsweise Zugriffskontrollkonzepte auf der Basis entsprechenden Strategien organisationsseitig definiert und technisch mit entsprechenden Zugriffskontrollsystemen umgesetzt. Unter dieser Kategorie werden zudem auch bauliche Maßnahmen subsumiert, die z.B. die Sicherung von Gebäuden oder Räumen betreffen. Rechtliche Maßnahmen, die mit einer rechtlichen Durchsetzbarkeit einhergehen, stellen die dritte Kategorie dar und betreffen z.B. Verträge mit Partnern oder externen Dienstleistern sowie Vereinbarungen zu Datenschutz oder Geheimhaltung mit den Mitarbeitern.

Neben der Unterscheidung in organisatorisch, technisch und rechtlich, können Steuerungsmaßnahmen auch den entsprechenden Wissensrisikoursachen Verlust, unerwünschte Diffusion, unzureichender Transfer und eingeschränkte Qualität zugeordnet werden. Wie bereits in Abschnitt 5.9.4 erwähnt, folgt die Steuerung von Wissensrisiken primär einem präventiven Ansatz, um Bewertungsprobleme zu kompensieren. Auf der anderen Seite reichen präventive Maßnahmen nicht aus, um Wissensrisiken effizient zu steuern. Demzufolge werden nachfolgend auch reaktive Maßnahmen erläutert. Daraus ergibt sich als weiteres Klassifikationskriterium eine Unterscheidung in reaktive und präventive Steuerungsmaßnahmen. Wie in Abschnitt 3.5.4 erörtert, bestehen im RM die potentiellen Handlungsalternativen Vermindern, Vermeiden, Überwälzen, Teilen und Akzeptieren, wobei letztgenannte Alternative keine Maßnahmen umfasst und somit im Folgenden nicht betrachtet wird. Die verbleibenden vier Handlungsalternativen können zu einer weiteren Spezifikation der Steuerungsmaßnahmen herangezogen werden. In Tab. 13 sind die verschiedenen Kriterien zur Klassifikation von Steuerungsmaßnahmen nochmals zusammengefasst. Dabei wird für die nachfolgenden Ausführungen die Dimension Maßnahmenart als primäres Gliederungselement herangezogen.

Maßnahmenart	organisatorisch		technisch		rechtlich	
Wissensrisikoursache	Verlust	unerwünschte Diffusion		unzureichender Transfer		eingeschränkte Qualität
zeitlicher Fokus	präventiv			reaktiv		
Handlungsalternative	Vermeidung	Verminderung		Überwälzung		Teilung

Tab. 13 Klassifikation der Steuerungsmaßnahmen

Eine integrierte Betrachtung verschiedener Konzepte zur Sicherheit wie sie durch Lux und Peske (2002, 170ff) im Hinblick auf die Abwehr von Wirtschaftsspionage und Competitive Intelligence vorgenommen wird, kann auch auf die Steuerung von Wissensrisiken übertragen werden (siehe Abb. 27). Demnach setzt Sicherheit in Bezug auf Wissensrisiken einerseits implementierte klassische Sicherheitsmaßnahmen voraus, die beispielsweise die Abwehr von Betriebskriminalität, Personenschutz, Schutz von Gebäuden gegen Einbruch und Brand etc. betreffen. Andererseits sind auch Maßnahmen im Bereich des IT-Sicherheitsmanagements als Voraussetzung anzusehen. Diese betreffen beispielsweise den allgemeinen Datenschutz, die regelmäßige Wartung der IT-Systeme, die Sicherung der IT-Systeme gegen unautorisierten Zugriff etc. Darauf basierend können Steuerungsmaßnahmen für Wissensrisiken ergriffen werden, die die darunter liegenden Sicherheitskonzepte entsprechend detaillieren und diese somit erweitern. Das Potential von Wissensrisiken ist demnach umso höher, je weniger ausgeprägt die Sicherheitsmaßnahmen auf allen drei Ebenen sind.

Bedingt durch die Anleihen aus den IT-RM und den Ansätzen zur Abwehr von Wirtschaftsspionage werden bei der nachfolgenden Erörterung von Steuerungsmaßnahmen auch Maßnahmen aus diesen Forschungsfeldern entliehen, wenn sie für den Untersuchungsgegenstand von Relevanz sind bzw. eine entsprechende Adaption im Sinne einer Erweiterung erforderlich ist. Insbesondere in Bezug auf das IT-RM erfolgt diese Entleihung allerdings nur auf einer sehr generischen Ebene, da umfassende und sehr detaillierte Standards in diesem Themenkomplex bestehen, auf die an dieser Stelle verwiesen wird. Folgt man der in Abschnitt 2.2.1 dargestellten Unterscheidung zwischen Daten, Informationen und Wissen[207], so stellen RM-Maßnahmen in Bezug auf die beiden erstgenannten Kategorien vielfach eine Voraussetzung bzw. die Basis für die Steuerung von Wissensrisiken dar. Es ist jedoch nicht davon auszugehen, dass Maßnahmen aus diesen beiden Bereichen durchgängig in Unternehmen implementiert sind und folglich der Erwartungswert von Wissensrisiken durch Mängel in diesen beiden Bereichen erhöht wird. Aus diesen Gründen fokussieren die nachfolgenden Betrachtungen zu Steuerungsmaßnahmen primär auf die oberste Ebene (siehe Abb. 27), wobei auch Maßnahmen in Bezug auf klassische Sicherheit und IT-Sicherheit erörtert werden, wenn sie entweder von besonderer Relevanz sind oder eine entsprechende Adaption auf Wissensrisiken erforderlich ist.

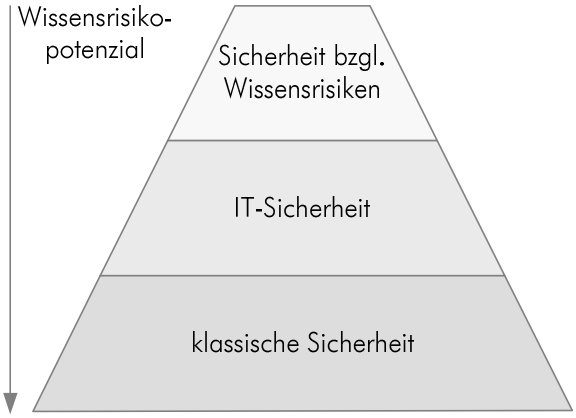


Abb. 27 Sicherheit in Bezug auf Wissensrisiken

Die Steuerungsmaßnahmen sind nicht immer ganz trennscharf, da insbesondere organisatorische Maßnahmen mit technischen und rechtlichen Maßnahmen zusammenhängen bzw. eine Voraussetzung für diese darstellen. Auch in diesem Fall wird wie bei der primären Ursachenzuordnung bei Wissensrisiken (siehe Abschnitt 5.2) eine Steuerungsmaßnahme derjenigen Kategorie zugewiesen, die den Schwerpunkt aufweist.

5.10.2 Organisatorische Steuerungsmaßnahmen

Im Rahmen dieses Abschnittes werden die identifizierten organisatorischen Steuerungsmaßnahmen dargestellt. Die Maßnahmen basieren auf einer Literaturanalyse, die als Managementansätze bzw. Forschungsgebiete u.a. den Disziplinen WM, strategisches Management, Wirtschaftsspionage und Personalmanagement zuzuordnen sind.

[207] Siehe hierzu Abschnitt 2.2.1.

Zur Steuerung von Wissensrisiken lassen sich für verschiedene Teilaspekte in Bezug auf erwartetes Mitarbeiterverhalten Richtlinien definieren, wobei allerdings die alleinige Definition der Richtlinien nicht ausreicht, sondern das Ergreifen weiterer Schritte erfordert, die auch in nachfolgender Abb. 28 zusammengefasst sind. Vielmehr ist auch deren entsprechende Kommunikation an die Mitarbeiter und gegebenenfalls die Durchführung von Trainingsmaßnahmen bzw. Schulungen erforderlich, um Klarheit darüber zu schaffen, welches Verhalten bzw. welche Anpassungen der Abläufe von den Mitarbeitern erwartet werden. Eine derartige Kommunikation schließt auch das in Aussichtstellen negativer Sanktionen ein, die eintreten, wenn die Richtlinien nicht eingehalten werden. Allgemeine Maßnahmen zur Sensibilisierung für bestimmte sicherheitsrelevante Aspekte sind auch Gegenstand der Kommunikation (Fox 2003, 678f; Verfassungsschutz 2004a, 7; BSI 2006, 1420ff; Niedermeier, Huth 2006, 18). Ziel muss es dabei immer sein, dass für die Mitarbeiter transparent ist, warum diese Anforderungen an sie gestellt werden, da dies die Akzeptanz von Sicherheitsmaßnahmen allgemein und -richtlinien im Speziellen verbessert (Maier 1992, 86). Neben der Kommunikation sind auch eine entsprechende Kontrolle der Einhaltung der Regelungen und gegebenenfalls das Ergreifen entsprechender Regulierungs- bzw. Durchsetzungsmaßnahmen erforderlich. Zudem ist eine Überprüfung der Wirksamkeit der Maßnahmen und ihrer Aktualität erforderlich, um laufend eine effektive Steuerung zu ermöglichen. Besteht Anpassungsbedarf z.B. aufgrund identifizierter Schwachstellen oder bedingt durch Innovationen erfolgt eine Adaption der Regelungen, was wiederum eine entsprechende Kommunikation und Kontrolle erforderlich macht. Organisatorische Richtlinien zu Sicherheitsaspekten wirken allgemein dem Risiko unzureichender Sicherheitsrichtlinien (VO7, DO3) entgegen und weisen verschiedene Gegenstände auf, die zur Steuerung spezifischer Wissensrisiken beitragen und nachfolgend erläutert werden[208].

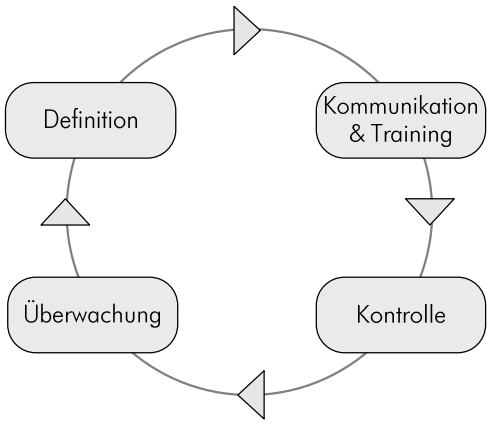


Abb. 28 Regelkreis zum Einsatz organisatorischer Richtlinien

- **Richtlinien zur Nutzung von IT-Systemen (SO1):** Verbindliche Richtlinien können sich darauf erstrecken, welche Sicherheitsmaßnahmen seitens der Mitarbeiter zu ergreifen sind, wenn sie IT-Systeme des Unternehmens nutzen. Dazu kann eine spezifische PC-Richtlinie erlassen werden oder entsprechende Klauseln in andere Richtlinien integriert werden. Neben Definitionen, Geltungsbereich, Rechtsvorschriften und Ansprechpartnern sind die zu ergreifenden Maßnahmen zentraler Gegenstand. Diese betreffen dabei im Speziellen Anmeldung an PCs, Verhaltensregeln bei Internetnutzung, Einsatz von Verschlüsselungsverfahren etc. Neue Benutzer sollten dabei erst

[208] Diese Aussagen gelten v.a. für die Steuerungsmaßnahmen SO1-SO7.

nach Bestätigung der Richtlinie die entsprechenden IT-Systeme nutzen dürfen. Bei Änderungen an den Inhalten (z.B. Einsatz neuer Sicherheitssysteme oder abweichende Sicherheitsanforderungen) der Richtlinien sollte eine erneute Bestätigung durch die Mitarbeiter eingefordert werden (BSI 2006, 964f). Speziell kann die Nutzung auch durch eine Datenschutzerklärung und die Verpflichtung der Mitarbeiter zur Einhaltung des Datensicherungskonzeptes einhergehen (BSI 2006, 988). Auf diese Weise kann eine Vorschrift zur ausschließlichen Nutzung von Netzlaufwerken sein, die in regelmäßigen Abständen (im Rahmen des Datensicherungskonzeptes) einem Backup unterzogen werden. So kann im Vergleich zur lokalen Sicherung von Inhalten bedingt durch Redundanzen das Risiko eines Wissensverlustes durch Löschung oder Datenverlust reduziert werden.

Als spezifischer Teilaspekt der Nutzung von IT-Systemen kann die Nutzung von Passwörtern geregelt sein. So können beispielsweise eine Mindestlänge von acht Zeichen und die Verwendung von Groß-, Kleinbuchstaben und Ziffern vorgeschrieben sein, um Entschlüsselungsversuche zu erschweren. Zudem können Aktualisierungszyklen definiert werden, zu denen die Mitarbeiter ihre Passwörter wechseln müssen, wobei eine erhebliche Abweichung vom vorherigen Passwort eingefordert werden kann. Darüber hinaus kann eine sofortige Änderung bei Vorliegen des Verdachtes, dass weitere Personen Kenntnis über das Passwort erlangt haben, vorgeschrieben sein. Der Anstoß dieser Aktualisierungen kann dabei auch durch systemseitige Erinnerungen unterstützt werden. Darüber hinaus kann auch die Geheimhaltung von Passwörtern geregelt sein. Erstgenannter Punkt schließt dabei insbesondere auch die Weitergabe von Passwörtern im Rahmen von Social Engineering Versuchen ein. Darüber hinaus kann auch eine Passwortsperrung des Rechners beim Verlassen des Arbeitplatzes eingefordert werden, um eine Benutzertrennung[209] zu gewährleisten und so das Diffusionspotential bzgl. eines unautorisierten Zugriffs zu reduzieren (Maier 1992, 122f; Bitkom 2003, 26; Yapp 2003, 175f; Ernst&Young 2004, 11; Kruth 2004, 200; Verfassungsschutz 2004a, 19; BSI 2006, 948f; Upadhyaya et al. 2006, 795).

- **Richtlinien zum Verlassen des Arbeitsplatzes (SO2)**: Gegenstand einer organisatorischen Richtlinie können zu ergreifende Maßnahmen beim Verlassen des Arbeitsplatzes sein. Zum Teil werden diese Maßnahmen auch als Clean Desk Policy bezeichnet, durch die die Mitarbeiter dazu verpflichtet werden, keine sensitiven Unterlagen offen auf den Schreibtischen liegen zu lassen sowie Datenträger oder physische Dokumente sicher (z.B. in abgeschlossenen Schränken) zu verwahren (BSI 2006, 882, 984; Meissinger 2006, 101). Dadurch soll verhindert werden, dass unau-

[209] Der Umgang mit Passwörtern und insbesondere die Benutzertrennung kann Gegenstand von Kontrollen sein. So kann mittels Auswertung der Protokollierung geprüft werden, ob eine Anmeldung durch die Nutzer erfolgt oder mehrere Mitarbeiter unter denselben Zugangsdaten angemeldet sind. Werden Verstöße festgestellt, so sollten die Mitarbeiter auf die Einhaltung der entsprechenden Richtlinien hingewiesen und die Bedeutung der Maßnahmen erneut vermittelt werden (BSI 2006, 1023).

torisierte interne oder externe Personen Kenntnis nehmen und dies die Basis für eine unerwünschte Diffusion darstellen kann.

- **Richtlinien zur Löschung und Vernichtung von Datenträgern und Dokumenten (SO3):** Als weiterer Gegenstand organisatorischer Richtlinien können Mitarbeiter dazu verpflichtet werden, sensitive Datenträger bzw. Dokumente professionell zu löschen (z.B. ordnungsgemäße Formatierung) oder zu entsorgen, um so zu verhindern, dass unautorisierte Dritte Kenntnis erlangen. Hinsichtlich physischer Dokumente kann so verhindert werden, dass sich unautorisierte Personen Zutritt zu Papierkörben im Bürogebäude oder bei sonstigen Entsorgungsstationen verschaffen (BSI 2006, 1331ff; Meissinger 2006, 102; Peltier 2006, 10f). Im Falle von Datenträgern kann die Löschung bei der Nutzung fremder PCs oder Datenspeicher sowie im Falle der Übermittlung eines PCs zur Reparatur an externe Dienstleister erforderlich sein. Das Erfordernis einer derartigen Vernichtung kann sich dabei an der Klassifikation des Wissens (siehe Abschnitt 5.9.1) orientieren und je nach Sicherheitsstrategie des Unternehmens nur für Inhalte, die nach einer höheren Sicherheitsstufe klassifiziert sind, erforderlich sein (Dreger 1998, 362).
- **Richtlinien zum Verhalten bei mobiler Arbeit (SO4)**: Ein weiterer Regelungsbereich betrifft den Umgang mit sensitiven Inhalten bei mobiler Arbeit, die Dienstreisen und Telearbeit umfasst, da gerade in diesen Situationen bedingt durch eine erhöhte Diebstahlsgefahr ein hohes Risikopotential in Bezug auf eine unerwünschte Diffusion besteht. Vielfach kommt dabei der Unachtsamkeit der Mitarbeiter eine besondere Bedeutung zu. Erforderliche Maßnahmen können beispielsweise die Aufbewahrung oder Sicherung von Notebooks (z.B. durch Notebookschlösser) sowie weitere mobile Endgeräte (z.B. Smartphones), Speichermedien und Dokumenten betreffen (BSI 2006, 882). Dabei können die Richtlinien auch verschärft werden, wenn Mitarbeiter Dienstreisen in bestimmte Länder, die aus der Sicht der Unternehmung ein größeres Risikopotential aufweisen, unternehmen (Desouza, Vanapalli 2005, 86f). Falls eine sichere Aufbewahrung sensitiver Inhalte nicht gewährleistet werden kann, sollte auf deren Mitnahme, wenn möglich, verzichtet werden (McGonagle, Vella 1994, 298). Falls ein Verlust eines Endgerätes eintritt, sollten die Mitarbeiter zudem zu einer sofortigen Meldung des Verlustes verpflichtet werden, damit Zugangsdaten umgehend gesperrt werden können und sonstige Maßnahmen, wie z.B. Berichterstattung an Kunden, ergriffen werden können (BSI 2006, 1736). Zudem kann vor einer Dienstreise überprüft werden, ob bestimmte Inhalte erforderlich sind oder nicht und so das Risikopotential durch Reduktion der Inhalte reduziert werden[210].

  Spezielle Richtlinien oder Klauseln können sich auch auf den Einsatz von Mobiltelefonen bezie-

[210] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, wird das Sicherheitsbewusstsein der Mitarbeiter in Bezug auf die mobile Sicherheit von 20% der befragten IT-Manager als gut, von 36% als indifferent und in 44% der Fälle als schwach eingestuft (Vile 2007, 5).

hen. Dabei sind neben allgemeinen Fragen wie Speicherung der Verbindungsdaten oder private Nutzung etc. insbesondere Maßnahmen in Bezug auf den Abhörschutz relevant, die verschiedene Verschlüsselungsverfahren einsetzen (BSI 2006, 1394ff)[211].

- **Richtlinien zur Meldung von Sicherheitsvorfällen (SO5)**: Weiterhin kann eine Meldung von Sicherheitsvorfällen vorgeschrieben sein. So kann eine derartige Meldung beispielsweise dann erforderlich werden, wenn sensitive Inhalte gestohlen wurden, externe Aushorchungsversuche erfolgt sind oder sonstige Auffälligkeiten beobachtet werden (Norman 2001, 52f). Eine effiziente Berichterstattung setzt dabei allerdings eine entsprechende Sensibilisierung der Mitarbeiter voraus und kann als Ergänzung zu weiteren Steuerungsmaßnahmen gesehen werden, die Richtlinien zur Nutzung von IT-Systemen (siehe SO1) oder zum Verhalten bei mobiler Arbeit (siehe SO4) betreffen.
- **Wissenstransferrichtlinien (SO6)**: Basierend auf der Klassifikation von Wissen und in Abstimmung mit potentiellen Kooperationsvereinbarungen können interne Wissenstransferrichtlinien als organisatorische Steuerungsmaßnahme definiert werden, die einerseits Risikopotentiale einer unerwünschten Diffusion begrenzen und andererseits den Erfolg des Wissenstransfers verbessern sollen, indem sie Klarheit darüber schaffen, inwiefern Wissen transferiert werden kann oder nicht (Hamel et al. 1989, 138f; Das, Teng 1999, 55f; Jordan, Lowe 2004, 256; Kratzke 2006, 204ff). Ebenso wie organisatorische Richtlinien allgemein ist eine leistungsfähige Implementierung der Wissenstransferrichtlinien und deren Kommunikation an die Mitarbeiter erforderlich (Fleischer 1997, 237). Im Falle von Kooperationen kann sich der Wissenstransfer auf Wissen beziehen, das die Kernkompetenzen nicht tangiert, um so Risiken, die mit einer potentiellen Entwertung aufgrund von Nichtexklusivität einhergehen, zu reduzieren. Dennoch sollte das transferierte Wissen auch für den Partner werthaltig sein, da sonst unter Umständen die Gegenleistungen des Partners vergleichsweise gering sind und somit die Potentiale des Wissenstransfers nicht ausgeschöpft werden (Lorange, Roos 1992, 352).
- **Richtlinien zu Auskünften und Publikationen (SO7)**: Ebenfalls auf der Basis einer Klassifikation von Wissen können Richtlinien in Bezug auf die externe Publikation oder Auskünfte als Steuerungsmaßnahme eingesetzt werden. So sind im Einzelnen die allgemeine Öffentlichkeitsarbeit im Sinne von Interviews, Pressekonferenzen, wissenschaftliche Publikationen in Fachzeitschriften (z.B. zu aktueller Forschung und Entwicklung), Auskünfte bei Umfragen, Auskünfte an potentielle Geschäftspartner oder die Abgabe von Angeboten an Kunden betroffen (Amelingmeyer 2002, 154; McGonagle, Vella 2004, 294ff). Bei bisher unbekannten Geschäftspartnern oder sonstigen Personen, die erstmals mit dem Unternehmen in Kontakt treten, kann zu-

[211] Siehe hierzu auch die Ausführungen zur Steuerungsmaßnahme Einsatz von Verschlüsselungsverfahren ST4 in Abschnitt 5.10.3.

dem eine Rückversicherung beim entsprechenden Unternehmen oder der jeweiligen Behörde erfolgen, um sicherzustellen, dass es sich tatsächlich um einen Mitarbeiter handelt und nicht eine falsche Identität vorgespiegelt wurde (BSI 2006, 2008). Das zentrale Ziel dieser Richtlinien besteht darin, zu verhindern, dass sensitive Inhalte über die Grenzen des Unternehmens diffundieren und somit eine potentiell gewinnbringende Nutzung durch Dritte erfolgen kann. Dabei ist es auch entscheidend auf den Gesamtzusammenhang der Publikationen und Auskünfte zu achten, da Dritte oder Konkurrenten im Speziellen durch gezielte Konkurrentenanalyse und Integration der verschiedenen Quellen eine Rekonstruktion sensitiver Inhalte vornehmen können. Aus diesem Grund ist es für eine leistungsfähige Steuerung in diesem Bereich erforderlich, dass zentrale Richtlinien dezentral einheitlich umgesetzt werden. Um die Kontrolle effizient durchführen zu können, ist es zudem bedeutend zu identifizieren, welche Themengebiete für Konkurrenten von Relevanz sind und welche Mittel von diesen eingesetzt werden, um an die Inhalte zu gelangen. Dabei kann neben einer vollkommenen Zurückhaltung bestimmter Inhalte auch eine gezielte Verschleierung oder Vagheit eingesetzt werden und beispielsweise auf die konkrete Angabe zu Personen, Produkten oder Technologien verzichtet werden (Barth 2001, 3f).

- **Führung (SO8):** Die Effizienz der Steuerung von Wissensrisiken hängt aufgrund des starken Personenbezugs von Wissen vom Verhalten der Mitarbeiter ab. Demzufolge ist eine entsprechende Integration wissensrisikoorientierter Aspekte in die Führung der Mitarbeiter bedeutend. Führung schließt in diesem Kontext die Kommunikation des erwarteten Verhaltens an die Mitarbeiter, das Aufzeigen von Anreizen und potentiell negativer Sanktionen, die Kontrolle der Umsetzung der Richtlinien, die Bewertung der Mitarbeiterleistung sowie das Ergreifen von verhaltensregulierenden Maßnahmen ein (McGonagle, Vella 1994, 299; Norman 2001, 52ff; Desouza, Vanapalli 2005, 92ff). Dabei kommt auch dem Vorleben des erwarteten Verhaltens bzw. einer Vorbildfunktion der Führungskräfte eine bedeutende Rolle zu (Verfassungsschutz 2004b, 8; Meissinger 2006, 99). Neben der Kommunikation des erwarteten Verhaltens und der Durchsetzung dieser Erwartungen kommt der Führung auch in Bezug auf die gezielte Beeinflussung der Fluktuationsneigung der Mitarbeiter ein besonderer Stellenwert zu. So können zum einen im Rahmen von Mitarbeitergesprächen individuelle Zielstellungen der Mitarbeiter identifiziert werden und auf dieser Basis deren Realisierung im Kontext der unternehmensspezifischen Zielstellungen fokussiert werden. Zum anderen kann die Arbeitszufriedenheit und somit die Fluktuationsneigung durch einen entsprechenden Führungsstil und eine entsprechende Anerkennungspolitik im Sinne des Unternehmens beeinflusst werden (Maier 1992, 91ff).
- **Auswahl der Mitarbeiter (SO9)**: Ebenso wie Richtlinien oder die Schaffung von Rollen stellt auch die gezielte Auswahl von Mitarbeitern eine Maßnahme dar, die die vier Wissensrisikoursachenkategorien übergreift und das Risikopotential begrenzt. So ist bei der Auswahl der Mitarbeiter

das Vorhandensein bestimmter Kompetenzen, die allgemein zur Durchführung wissensintensiver Aufgaben erforderlich sind, zu überprüfen. Darüber hinaus sollten auch spezifische Kenntnisse im Umgang mit IT-Systemen und im Speziellen mit Sicherheitstechnologien ebenfalls Gegenstand dieser Überprüfung sein, um sicherzustellen, dass diese Aufgaben auch unter Beachtung von Sicherheitsaspekten durchgeführt werden können (Abell, Oxbow 2002, 128ff; BSI 2006, 491). Dazu können zertifizierte Leistungen bzw. Zeugnisse eingefordert werden. Können diese Kenntnisse im Zuge der Personalauswahl nicht vollständig überprüft werden, so sollte eine Überprüfung in der Frühphase des Arbeitsverhältnisses vorgenommen werden und potentiell identifizierte Lücken durch gezielte Personalentwicklungsmaßnahmen geschlossen werden. Neben Kompetenzen sollten auch charakterliche Eigenschaften und insbesondere die Vertrauenswürdigkeit der potentiellen Mitarbeiter im Rahmen der Personalauswahl einer Überprüfung unterzogen werden, um insbesondere Risikopotentiale in Bezug auf die unerwünschte Diffusion und den Verlust von Wissen zu begrenzen. Dazu können die Bewerbungsunterlagen auf ihre Echtheit und Schlüssigkeit überprüft, Arbeitszeugnisse im Hinblick auf Fehlverhalten interpretiert, ehemalige Arbeitgeber kontaktiert oder Informationen aus sonstigen externen Quellen (z.B. polizeiliches Führungszeugnis, Kontakt zu Nachrichtendiensten) eingeholt werden (Maier 1992, 68ff; Dreger 1998, 370ff; Verfassungsschutz 2004b, 12)[212]. Diese Auswahlkriterien können dabei auch bei der Auswahl externen Personals, das kurzfristig eingesetzt wird, herangezogen werden. Neben der Auswahl neuer Mitarbeiter kann auch eine gezielte Besetzung von Rollen in Bezug auf Kooperationen, das Risikopotential reduzieren (Das 2005, 715).

- **Mitarbeiterbindung (SO10):** Um der Fluktuation von Mitarbeitern und dem damit einhergehenden Verlust von Kompetenzen und Erfahrungswissen entgegenzuwirken, können verschiedene Maßnahmen ergriffen werden, um die Mitarbeiter an das Unternehmen zu binden bzw. deren Fluktuationsneigung zu reduzieren (Knaese, Probst 2001, 36; Kobi 2003, 108). Die Bindungswirkung der Mitarbeiter wird durch eine Reihe an monetären und nicht monetären Einflussfaktoren beeinflusst und kann zusammenfassend als akquisitorisches Potential bezeichnet werden (Drumm 2000, 335). So ist zum einen die Vergütung als monetärer Faktor von Bedeutung und muss interorganisatorischen Vergleichen standhalten, um Bindungswirkung zu entfalten. Dazu zählen auch die Sozialleistungen des Unternehmens und variable Anteile. Weitere Einflussfaktoren stellen z.B. die Reputation des Unternehmens, das Betriebsklima, die Art der Aufgaben, die Machtverteilung oder die Entwicklungsmöglichkeiten dar (Bonora, Revang 1993, 205ff; Kobi 1999, 82; Amelingmeyer 2002, 151). Eine detaillierte Analyse von Einflussfaktoren wurde von Knaese durchgeführt.

[212] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, nehmen ca. 1/3 der beteiligten Unternehmen mit mehr als 5000 Mitarbeitern und 1/4 der Unternehmen zwischen 500 und 5000 Mitarbeitern explizit eine Überprüfung sicherheitsrelevanter Fragestellungen bei der Auswahl und Einstellung der Mitarbeiter vor (Collins, Vile 2007, 5).

Als besonders relevant stellten sich in dieser Studie die Faktoren Arbeitsinhalt (z.B. abwechslungsreiche Aufgaben), Entwicklungsmöglichkeiten (z.B. Karriereoptionen), Verantwortung (z.B. Führungsaufgaben), Strategie (z.B. Entwicklungsperspektiven des Geschäftsbereiches), Arbeitsorganisation (z.B. Entscheidungsstrukturen) und Vernetzung (z.B. soziales Umfeld) heraus (Knaese 2004, 226ff)[213]. Zur Evaluation der Fluktuationsneigung der Mitarbeiter können fluktuationsrelevante Faktoren einen Erhebungsgegenstand von Mitarbeitergesprächen oder -befragungen darstellen. Auf der Basis dieser Erkenntnisse können entsprechende Maßnahmen eingeleitet werden, um die Bindungswirkung zu erhöhen (Kobi 1999, 78ff). So können auf dieser Basis den Mitarbeitern z.B. gezielte Veränderungen der Arbeitsinhalte, Weiterbildungen oder variable Zusatzleistungen geboten werden. Dabei sollte bei der Ergreifung von Bindungsmaßnahmen im monetären Bereich die Vergütung von vergleichbaren Stellen bei Konkurrenzunternehmen einbezogen und daher in regelmäßigen Abständen erhoben werden.

- **Maßnahmen beim Ausscheiden der Mitarbeiter (SO11)**: Um Risiken des Verlustes und der Diffusion entgegenzuwirken, sollten beim Ausscheiden der Mitarbeiter Maßnahmen ergriffen werden. Diese betreffen die Rückgabe von Notebooks, Speichermedien, Mitarbeiterkarten, Schlüssel sowie physische Dokumente, die von einer Erklärung begleitet werden kann, mittels derer die Rückgabe des gesamten Unternehmenseigentums versichert wird. Zudem sind die Zutritts- und Zugriffsberechtigungen (siehe ST5 und ST6 in Abschnitt 5.10.3) zu entziehen und Vertreterregelungen anzupassen. Darüber hinaus sollten ggf. Sicherheitsverantwortliche und Geschäftspartner darüber informiert werden, dass der Mitarbeiter nicht mehr für das Unternehmen tätig ist und dementsprechend über keinerlei Vollmachten verfügt. Bei Bekanntwerden des Ausscheidens sollte zudem bis zum endgültigen Austritt auf Auffälligkeiten, wie z.B. Kontakte zu Wettbewerbern, erhöhte Sammlung von Kopien etc. geachtet werden und ggf. eine sofortige Entbindung von sicherheitsempfindlichen Aufgaben vorgenommen werden. Vor dem endgültigen Ausscheiden sollte der Mitarbeiter darauf hingewiesen werden, dass die getroffenen Geheimhaltungsvereinbarungen weiterhin wirksam sind (Dreger 1998, 370ff; Verfassungsschutz 2004a, 7; BSI 2006, 2020f; Meissinger 2006, 88)[214].
- **Personalentwicklung (SO12)**: Ebenso wie die gezielte Personalauswahl ist auch die Entwicklung der Mitarbeiter eine konzeptübergreifende Maßnahme, die zu einer Reduktion der Risikopotentiale positiv beiträgt. Ziel ist es dabei, diejenigen Fach-, Methoden- und Sozialkompetenzen, die zur Verfolgung der Unternehmensziele beitragen, durch gezielte Maßnahmen auf ein erwünschtes Ni-

[213] Für weitere Details siehe (Knaese 2004).

[214] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, bestehen bei 44% der beteiligten Unternehmen auf physische und IT-Sicherheit fokussierte Richtlinien bzw. Verfahrensanweisungen in Bezug auf die Einstellung, den Arbeitsplatzwechsel und den Austritt der Mitarbeiter (Collins, Vile 2007, 6).

veau zu heben (Drumm 2000, 382). So ziehen insbesondere veränderte Qualifikationsanforderungen in volatilen Themengebieten, wie z.B. IT oder Pharmazie, ebenso wie Anforderungen in Bezug auf IT-Sicherheitsmaßnahmen einen erhöhten Entwicklungsbedarf nach sich. Die Entwicklung der Mitarbeiter kann auch darauf abzielen, Werthaltungen in Bezug auf den Umgang mit sensitiven Inhalten zu etablieren (Liebeskind 1997, 635). Des Weiteren kann eine gezielte Schulung der Mitarbeiter in Bezug auf die Nutzung von IT-Systemen bzw. entsprechender Anwendungen oder Funktionalitäten mit besonderer Wichtigkeit erfolgen, um Risiken, die sich aus einer unsachgemäßen Nutzung ergeben, zu vermindern. So kann die Vermittlung von Kenntnissen beispielsweise in Bezug auf die Nutzung von Sicherheitstechnologien, das Verhalten bei eintretenden Sicherheitsvorfällen, den Umgang mit Passwörtern, das Verhalten bzw. Erkennen von Social Engineering Versuchen oder das Ergreifen von Notfallmaßnahmen betreffen (BSI 2006, 2016ff).

- **Redundanzschaffung (SO13):** Im Hinblick auf die Kompensierung von Wissensverlusten und die Verbesserung der Wissensqualität durch die Reduktion von Abhängigkeiten können als Steuerungsmaßnahme gezielt Redundanzen geschaffen werden (Güldenberg 1997, 270). Dieses Erfordernis ergibt sich primär aus den verschiedenen Formen der Fluktuation und einem möglichen Personalausfall (siehe Abschnitt 5.3.1). So kann eine erhöhte Verteilung von Kompetenzen beispielsweise durch eine entsprechende Zusammenstellung von Teams, den Einsatz von Mentorenprogrammen oder Weiterbildungen durch Mitarbeiter selbst erreicht werden (Bonora, Revang 1993, 202f; Amelingmeyer 2002, 151f).
- **Einsatz von Genehmigungsprozessen (SO14):** Eine weitere Steuerungsmöglichkeit in Bezug auf die Reduktion des Risikopotentials einer unerwünschten Diffusion stellt die Definition von Genehmigungsprozessen, die eine Freigabe sensitiver Inhalte zum Gegenstand haben, dar. Die Verantwortlichkeit für derartige Prozesse können dabei von bestimmten Rollen übernommen werden. So werden durch den Einsatz von Gatekeepern Inhalte vor dem Transfer auf ihre Sensitivität hin überprüft (Hamel et al. 1989, 136; Fleischer 1997, 238; Loebbecke et al. 1999, 20; Awazu 2004b, 21). Dabei ist die Limitierung der Wissenstransferprozesse auf eine einzelne bzw. wenige Personen, die die Rolle des Gatekeepers ausüben, zum Teil nur schwer realisierbar, da aufgrund der Vielzahl der Themengebiete das erforderliche Detailwissen fehlt und dadurch eine solide Beurteilung nur schwer möglich ist. Daher kann alternativ eine Ausweitung auf mehrere Personen erfolgen (Norman 2001, 54). Genehmigungsprozesse stellen allerdings potentiell auch eine rigide Sicherheitsmaßnahme (TO5) dar, die den Erfolg des Wissenstransfers hemmen bzw. dessen Potentiale einschränken kann. Somit ist eine Abwägung erforderlich, inwieweit eine Einschränkung erfolgen soll.
- **Vier-Augen-Prinzip (SO15):** Als Steuerungsmaßnahme, die darauf fokussiert, den Missbrauch von Zugriffsrechten zu verhindern, kann das Vier-Augen-Prinzip eingesetzt werden. Dieses Prin-

zip setzt dabei voraus, dass nur zwei oder mehr Mitarbeiter bestimmte Aufgaben, wie z.B. Zugreifen, Ändern oder Löschen sensitiver Inhalte, vornehmen können. Dabei liegt dem Vier-Augen-Prinzip die These zugrunde, dass mit Zunahme der an der Aufgabe beteiligten Mitarbeiter die Wahrscheinlichkeit einer unautorisierten Handlung bzw. eines Missbrauchs der Rechte sinkt. Potentiell negative Auswirkungen auf das Betriebsklima sind jedoch auch in diesem Fall möglich, da Misstrauen erzeugt werden kann. Dieses Prinzip findet beispielsweise Anwendung im Bankenbereich, wenn eine Verifikation von Dateneingaben erfolgt, bei der die Eingaben der einen Person mit anderen Personen abgeglichen werden. Ein weiteres Anwendungsbeispiel stellen Administratorenrechte[215] von IT-Systemen dar (Maier 1992, 108f; van den Brink 2001, 8, 72). Im Hinblick auf die Wissensqualität kann das Vier-Augen-Prinzip auch einen positiven Beitrag zur Verbesserung leisten, indem beispielsweise Angaben mehrerer Mitarbeiter verifiziert werden. So kann z.B. die Korrektheit von Beiträgen durch andere Mitarbeiter bestätigt werden (Eppler 2004, 332).

- **Aufteilung von Wissen (SO16)**: Ähnlich zum Vier-Augen-Prinzip kann auch eine gezielte Aufteilung von sensitivem Wissen vorgenommen werden, um das Schadensausmaß der Diffusion zu reduzieren. So können beispielsweise Betriebsgeheimnisse, wie z.B. Rezepturen zur Herstellung von Produkten oder das Wissen über einen gesamten wertschöpfenden Prozess, nicht auf eine einzelne Person gebündelt sein, sondern eine Aufteilung auf mehrere Personen vorgenommen werden. Diese Verteilung ist ähnlich einer funktionalen Trennung von Aufgaben und Zuständigkeitsbereichen, wie sie vielfach im Bankenbereich oder in Bezug auf die Administration von IT-Systemen[216] vorgenommen wird. Dabei verfügen Mitarbeiter nur über tätigkeitsbezogenes Wissen und nehmen auch nur entsprechende Aufgaben wahr. Auf diese Weise kann das Schadensausmaß einer Diffusion begrenzt werden, da im Falle einer Interfluktuation keine vollständige Rekonstruktion des Wissens möglich ist (Feinstein, Stein 1988, 402; Rønde 2001, 393; van den Brink 2001, 7f). Eine derartige Trennung kann sich dabei aber negativ auf die unternehmensinterne Zusammenarbeit auswirken. Somit ist eine Abwägung zwischen der Erschwerung einer unerwünschten Diffusion und der potentiellen Hemmung interner Potentiale in Bezug auf die Zusammenarbeit erforderlich. Es erscheint daher zweckmäßig eine derartige Aufteilung nur in hoch sensitiven Bereichen vorzunehmen und in die Betrachtungen die aktuelle Wettbewerbsintensität und die Abwerbungsversuche von Konkurrenten einzubeziehen.
- **Dokumentation (SO17)**: Die gezielte Dokumentation von personenbezogenem Wissen wie Erfahrungen, die in Projekten oder im Tagesgeschäft gesammelt wurden, stellt eine weitere Steue-

[215] So kann die Administration der IT-Systeme als verteilte Rolle betrachtet werden, um die Konzentration auf einzelne Mitarbeiter zu reduzieren und Raum für opportunistische Nutzung der Rechte zu limitieren. Beispiele für Rollen sind Workgroup Manager, User Account Manager, File Server Console Operator (BSI 2006, 985).

[216] Beispiele für Funktionstrennungen sind Nutzerrechteverwaltung vs. Revision, Datenerfassung vs. Zahlungsanordnungsbefugnis (BSI 2006, 937).

rungsmaßnahme dar, die speziell Wissensverlusten, die sich aus dem Prozess des Vergessens ergeben, entgegenwirken. Dabei bestehen insbesondere in Bezug auf die Erfassung von Projektwissen verschiedene Ansätze, die beispielsweise zu bestimmten Meilensteinen oder am Projektende eine Dokumentation erforderlich machen. Beispiele sind Projekt De-Briefings, After Action Reviews oder Post-Project Appraisal (Disterer 2002, 517; Elsner 2002, 31f; Schindler, Eppler 2003, 221ff; Probst et al. 2006, 74). Im Tagesgeschäft kann beispielsweise die gezielte Anfertigung von Protokollen eingesetzt werden, um Wissen zu erfassen (Amelingmeyer 2002, 152). Speziell bezogen auf die Mitarbeiterfluktuation kann die Dokumentation auf der Basis von Austrittsgesprächen erfolgen, die auch Gegenstand von Nachfolgeregelungen (siehe SO18) sein können (Probst et al. 2006, 200f). Bei der Erfassung des personengebunden Wissens ist es dabei zentral, dass zum einen der mit der Dokumentation verbundene Aufwand möglichst gering ist, um die Akzeptanz der Mitarbeiter sicherzustellen und zum anderen der erfasste Kontext möglichst umfassend ist, um eine erhöhte Wiederverwendbarkeit im Sinne der Wissensqualität zu gewährleisten[217]. Um den für diesen Prozess erforderlichen Zeitaufwand gering zu halten, kann die Erfassung durch vorstrukturierte Dokumentationsvorlagen unterstützt werden. Die Vorlagen können beispielsweise auf einer verkürzten Form eines Mikroartikels basieren und die Elemente Thema, Story, Einsicht und Folgerungen beinhalten. Dabei stellt das Thema den Oberbegriff für die Erfahrung dar, während im Rahmen der Story eine kompakte Beschreibung des Lernanlasses und des konkreten Problems erfolgt (Willke 1998, 100ff). Dieses Element beschreibt den Kontext, in dem die Erfahrung gemacht wurde. Die Einsicht dient zur Dokumentation der Erkenntnis bzw. des Lerngrundes, z.B. die Ursache eines Problems, wobei Folgerungen dazu genutzt werden sollen, auf Basis der Einsicht konkrete Vorschläge oder Lösungsmaßnahmen niederzuschreiben. Durch eine derartige Strukturierung kann die Nachvollziehbarkeit der dokumentierten Erfahrungen verbessert werden. Um den Dokumentationsaufwand für die Nutzer möglichst gering zu halten, können IT-Systeme die Kontexterfassung unterstützen[218]. Ferner kann die Anwendung des dokumentierten Wissens beispielsweise technisch durch das Bereitstellen entsprechender Plattformen wie Foren oder Communities erfolgen. So wird bei McKinsey ein so genanntes Rapid Response Netzwerk eingesetzt, das Erfahrungen der Mitarbeiter zu Projekten enthält und auch die Kontaktierung der entsprechenden Autoren bzw. Projektmitarbeiter ermöglicht. Dabei werden Lessons Learned in regelmäßigen Abständen von den Projektmitarbeitern eingefordert und dann bereitgestellt (Probst et al. 2006, 74). Generell ist bei der Dokumentation von Wissen die Verhältnismäßigkeit des erforderlichen Aufwandes zu beachten, um nicht die Durchlaufzeit der Geschäftsprozesse durch diese Tätigkeiten zu stark einzuschränken. Darüber hinaus ist die Einbindung dokumentierten Wissens in

[217] Siehe hierzu auch Abb. 25 in Abschnitt 5.6.
[218] Siehe hierzu auch (Bayer et al. 2005; Maier, Bayer 2005).

die Prozesse erforderlich, damit auch eine Anwendung erfolgt. Mahnke weist in diesem Zusammenhang darauf hin, dass ein Trade-off zwischen dem Aufwand für die Dokumentation des Wissens und den in Kauf genommenen Verlusten besteht. Dabei bestehen auch Abstufungen wie spezifisch Wissen dokumentiert wird. Diese können von einfachen Hinweisen, bis hin zu umfassenden Prozessbeschreibungen mit umfangreicher Darlegung des Kontexts reichen. Somit gilt es, den potentiellen Verlusten die Kosten der Erstellung der Dokumentation gegenüberzustellen. Die direkten Erstellungskosten ergeben sich aus dem für die Dokumentation und die Sicherstellung der Anwendbarkeit des Wissens erforderlichen Zeitaufwand. Je impliziter der Gehalt des Wissens ist, umso höher ist der Aufwand. Zum Teil ist auch eine Kodifizierung impliziten Wissens nicht möglich, was entsprechende Auswirkungen auf den Aufwand hat. Diesem Aufwand müssen die Verluste gegenübergestellt werden, die sich daraus ergeben, dass Wissen nicht oder in geringerem Umfang dokumentiert wird. Diese Verluste ergeben sich beispielsweise aus der Abstrahierung oder dem Weglassen bestimmter Aspekte. Insgesamt sind bei der Dokumentation von Wissen die Anreize für die Mitarbeiter entscheidend (Mahnke 1999, 14f). Verluste, die sich aus der potentiellen Nichtdokumentation ergeben, sind in der Regel nicht prognostizierbar, da zum Entscheidungszeitpunkt Unsicherheit besteht, inwiefern das betroffene Wissen zukünftig Anwendungsbedarf haben wird oder nicht. Aus ökonomischen Gesichtspunkten sind somit bestimmte Themengebiete bzw. Kompetenzbereiche oder auch konkrete Anlässe wie Projektabschlüsse zu definieren, zu denen Dokumentationen eingefordert werden. Mangelnde Dokumentation von Wissen kommt noch stärker zum Tragen, wenn im Zuge der Fluktuation Wissensträger das Unternehmen verlassen. Aus diesem Grund ist gerade auch eine Dokumentation des für die Ausführung bestehender Tätigkeiten bzw. Stellen erforderliche Wissen bedeutend, da ansonsten bei der Nachbesetzung oder Vertretung des die Aufgabe bzw. Stelle ausführenden Mitarbeiters Einarbeitungsprobleme auftreten können (van den Brink 2001, 66; Knaese 2004, 43). Das dokumentierte Wissen kann dabei z.B. über Portale systematisch verbreitet bzw. zugreifbar gemacht werden.

- **Nachfolgerregeln (SO18):** Nachfolgerregelungen zielen darauf ab, fluktuationsbezogene Wissensrisiken zu reduzieren und v.a. die Einarbeitung der Stellennachfolger und den in diesem Zusammenhang erforderlichen Wissenstransfer möglichst effizient zu gestalten. Weit verbreitet sind Mentorensysteme, bei denen einem einzuarbeitenden Mitarbeiter ein anderer Mitarbeiter mit langjähriger Erfahrung im Unternehmen zur Seite gestellt wird (Amelingmeyer 2002, 152). Oftmals handelt es sich dabei um Mitarbeiter, die in naher Zukunft aus dem Unternehmen ausscheiden. Die erhöhte Effizienz der Einarbeitung und die Verminderung des Risikoerwartungswertes von Wissensverlusten kann dadurch erreicht werden, dass es bei der Einarbeitung zu einer Überlappung des bisherigen und des nachfolgenden Stelleninhabers kommt, da so auch Wissen transferiert wird, das über potentiell vorhandene stellenbezogene Dokumentationen hinausgeht (Probst et

al. 2006, 199f). Unabhängig von Mentorensystemen oder der Überlappung der Mitarbeiter kann die Dokumentation stellenbezogenen Wissens seitens des Unternehmens eingefordert werden.

- **Vertreterregeln (SO19):** Vertreterregelungen sind insbesondere im Falle eines Personalausfalls sowie für Urlaubszeiten und Dienstreisen erforderlich und sollen ein reibungsloses Ablaufen der Aufgaben in Prozessen / Projekten gewährleisten. Sie setzen voraus, dass der jeweilige Bearbeitungsstand der Aufgaben hinreichend dokumentiert ist, die Vertreter über die erforderlichen Kenntnisse verfügen und gegebenenfalls geschult werden sowie die zur Ausführung der Aufgaben erforderlichen Berechtigungen an den Vertreter übertragen werden. Dabei kommt auch einer gezielten Auswahl und frühzeitigen Einarbeitung der potentiellen Vertreter eine Bedeutung zu. Bei einer planbaren Vertretung empfiehlt es sich zudem, eine ordentliche Übergabe der Aufgaben zwischen Vertreter und Vertretenem vorzunehmen (BSI 2006, 2015).
- **Erhaltung informeller Netzwerke (SO20)**: Da durch häufige Reorganisationen in Bezug auf die Zusammensetzung von Teams, Abteilungen, Projektteams sowie unternehmensinterne Stellenwechsel Netzwerke zwischen den Mitarbeiter negativ beeinträchtigt werden, können Steuerungsmaßnahmen ergriffen werden, die auf die Aufrechterhaltung formeller und informeller Netzwerke abzielen (Amelingmeyer 2002, 151). So können beispielsweise Communities eingerichtet werden, um Netzwerke und somit Beziehungskapital aufrechtzuerhalten.
- **risikobewusste Auswahl des Kooperationspartners (SO21):** Im Hinblick auf den interorganisatorischen Wissenstransfer ist die gezielte Auswahl des Partners bedeutend, da sich Inkompatibilitäten negativ auf den Erfolg der Partnerschaft im Allgemeinen und den Wissenstransfererfolg im Speziellen auswirken können. Über die Anforderungen einer traditionellen Kooperation, die v.a. Strategie, Organisation und Kultur betreffen, hinausgehend sind im Falle von Kooperationen, die den Austausch und die Generierung von Wissen zum zentralen Gegenstand haben, Anforderungen in Bezug auf die Kompatibilität der Wissensbasen der Partner für den Erfolg des Wissenstransfers von Bedeutung. Dabei ist eine zunehmende Überschneidung der Kompetenzfelder der Partner förderlich, da bedingt durch ein so geschaffenes Grundverständnis die Aufnahme von Wissen des Partners erleichtert wird (Inkpen 2000, 1032). Ein gewisses Grundverständnis bzw. eine entsprechende Überlappung der Kompetenzen kann dabei sogar als Voraussetzung angesehen werden, da Kompetenzlücken die Rekontextualisierung des Wissens erschweren oder sogar unmöglich machen (Hamel 1991, 91; Hill, Hellriegel 1994, 594; Nielsen 2002, o.S.; Cummings, Teng 2003, 46f; Song et al. 2003, 355). Dabei können aber auch zu bestimmten Themen unterschiedliche Auffassungen und Einstellungen der Partner bestehen und somit der Wert eines gemeinsamen Grundverständnisses geschmälert werden. Auf der anderen Seite schränkt eine zu starke Überschneidung der Wissensbasen die Lernpotentiale für die Partner ein, wodurch Wissenstransfererfolg der Partnerschaft in Aggregation betrachtet negativ beeinträchtigt werden kann (Inkpen 2000, 1032).

Kooperationen sind generell durch das Grundproblem einer asymmetrischen Informationsverteilung gekennzeichnet. Speziell bei wissensintensiven Kooperationen kommt dies besonders zum Tragen, da der Wert des Wissens des Partners unklar ist (Aulinger 1996, 96). Die Partnerauswahl steht somit in Bezug auf die Kompatibilität der Wissensbasen in einem Spannungsfeld. Einerseits ist eine gewisse Überschneidung der Kompetenzen erforderlich, um ein Grundverständnis zwischen den Partnern sicherzustellen, während andererseits eine zu starke Überschneidung die Lerngelegenheiten und somit die Potentiale der Kooperation eingrenzt.

Zur Unterstützung der Partnerwahl können Anforderungen in Bezug auf die strategische Ausrichtung, die Organisation, die Kultur und die erforderlichen Kompetenzen definiert und im Rahmen der Kooperationsvorbereitung überprüft werden. Rissbacher schlägt dazu den Einsatz eines gewichteten Punkteschemas vor, auf dessen Basis Handlungsempfehlungen zur Eignung des Kooperationspartners im Hinblick auf den Beitrag zur Zielerreichung und unter Abwägung der Kosten und des Nutzens abgeleitet werden. Je nach Beitrag zur Zielerreichung können potentielle Kooperationspartnern gewählt werden oder von einer Zusammenarbeit Abstand genommen werden (Rissbacher 2003, 205ff).

Ebenso wie bei der Auswahl von Mitarbeitern können neben Kompetenzen und Leistungsfähigkeit des potentiellen Kooperationspartners auch charakterliche Eigenschaften Gegenstand des Auswahlprozesses sein und dabei insbesondere auch das Verhalten in anderen bzw. vorhergehenden Kooperationsbeziehungen evaluiert werden.

- **risikobewusste Auswahl von Outsourcing-Dienstleistern (SO22)**: Ebenso wie bei der Auswahl der Kooperationspartner kann auch die Auswahl externer Dienstleister und insbesondere Outsourcinganbieter wissensrisikoorientiert erfolgen und spezifische Kriterien zugrunde legen. Dies ist v.a. dann bedeutend, wenn externen Dienstleistern Zutritt zum Unternehmen oder Zugriff auf Anwendungen und sensitive Inhalte gewährt wird. Bei der Auswahl von externen Beratern, Zertifizierern etc. kann zudem darauf geachtet werden, dass diese nicht für direkte Konkurrenten tätig sind, um so die Diffusionspotentiale zu vermindern (BSI 2006, 2082; Meissinger 2006, 14). Die Auswahl kann sich dabei an den Ausführungen zur Auswahl von Kooperationspartnern (siehe SO21) orientieren.
- **Partnerbindung (SO23)**: Kooperationen gehen mit dem Risiko einher, dass Partner ihre Verhandlungsmacht ausnutzen und sich opportunistisch verhalten. Dieses Risikopotential kann reduziert werden, indem das Unternehmen seinerseits die Verhandlungsmacht erhöht, indem Abhängigkeiten geschaffen und Partner so gebunden werden. Derartige Abhängigkeiten ergeben sich beispielsweise aus getätigten kooperationsspezifischen Investitionen, die auf der Anschaffung gemeinsamer Produktionsanlagen, -standorte oder weiterer spezifischer Einrichtungen basieren. Bei Verlassen der Kooperation durch den Partner sind solche spezifischen Investitionen verloren

und stellen somit Umstellungskosten für den Partner dar, die auch das Abhängigkeitspotential erhöhen (Das 2005, 711). Weiterhin können solche Abhängigkeiten dadurch geschaffen werden, dass kritische Ressourcen ausgetauscht werden und somit gegenseitige „Geiseln" bestehen, die die Verwundbarkeit erhöhen und opportunistisches Verhalten begrenzen. Dabei ist allerdings eine regelmäßige Bewertung bzw. ein erneuter Austausch erforderlich, da sich deren Wert im Zeitablauf ändert (Nooteboom et al. 1997, 317; Das 2005, 712f). Darüber hinaus kann die auf einer Abhängigkeit des Partners basierende Reduktion der Wahrscheinlichkeit opportunistischen Verhaltens auch durch den Aufbau eines Reputationsdrucks reduziert werden, da so potentielles Fehlverhalten des Partners auch von anderen Wirtschaftsteilnehmern wahrgenommen wird und dies deren Verhältnis zum Partner negativ beeinträchtigen kann (Dyer, Nobeoka 2000, 358; Ford 2001, 556). Neben Zwängen bzw. Drohpotentialen können auch anreizorientierte Maßnahmen eingesetzt werden, um die Partnerbindung zu erhöhen. So kann beispielsweise in Aussicht gestellt werden, dass im Verlauf der Kooperation immer mehr werthaltiges Wissen transferiert wird (Fleischer 1997, 326). Zudem können partizipative Entscheidungsfindungen ebenfalls opportunistisches Verhalten unterdrücken und Bindungswirkung haben (Das 2005, 714). Sind die Abhängigkeiten zweiseitig, so besteht im Umkehrschluss auch für das Unternehmen das Risiko, dass mit dem Verlassen der Kooperation Umstellungskosten verbunden sind (Gahl 1991, 60). Somit muss eine Abwägung der Notwendigkeit der Bindung des Partners, die durch den Wert der eingebrachten wissensbezogenen Ressourcen bestimmt wird und der vom Unternehmen in Kauf genommenen Umstellungskosten erfolgen.

- **Kontrolle des Partners (SO24):** Zur Unterdrückung opportunistischen Verhaltens können zudem in Kooperationen Kontrollen eingesetzt werden (Das 2005, 713f). Dabei besteht generell ein Zusammenhang zwischen Kontrollmaßnahmen und Vertrauen. Während erstgenannte Maßnahmen formal durchgeführt werden und beispielsweise den Einsatz von Verträgen oder die Überwachung von Leistungen beinhalten, ist Vertrauen informeller Natur und hat gegenseitige Erwartungshaltung in Bezug auf soziale Normen und Werthaltungen, Pflichtgefühl oder Aufrichtigkeit zur Folge. Bestehendes Vertrauen stellt demnach eine informelle Kontrollmaßnahme dar, die auf Verhaltenserwartungen und deren Einhaltung basiert (Woolthuis et al. 2002, 3; Paik 2005, 494f). Somit können formale Kontrollen durch Vertrauen substituiert werden und umgekehrt. Dieser Zusammenhang ist aber mitunter problematisch, da umfassende Kontrolle Misstrauen an den Partner signalisiert und dies die Potentiale des Wissenstransfers negativ beeinträchtigen kann. Somit ist eine Abwägung zwischen den beiden Handlungsoptionen erforderlich. Anderseits kann auch eine beiderseitige Einigung auf eine formale Kontrolle erfolgen (Woolthuis et al. 2002, 8).
- **Begrenzung der personellen Interaktionspunkte (SO25)**: Eine organisatorische Steuerungsmaßnahme zur primären Verminderung des Risikopotentials einer unerwünschten Diffusion be-

steht darin, die Zahl der an der Kooperation beteiligten Mitarbeitern zu kontrollieren und so eine verbesserte Kontrollierbarkeit der externen Wissensflüsse zu erreichen (Baughn et al. 1997, 112; Norman 2001, 54). Dies kann auch so erfolgen, dass die Kooperation strukturell bzw. geographisch isoliert gestaltet wird und somit die Mitarbeiter des Partners nur mit den ausgewählten Mitarbeitern interagieren können (Liebeskind 1997, 650f; Das, Teng 1999, 55). Eine derartige Begrenzung vermindert einerseits die Risikopotentiale der Diffusion, kann aber andererseits auch die Erfolgspotentiale des Wissenstransfers limitieren, da umfangreiche Interaktion vorteilhaft für die De- und Rekontextualisierung des transferierten Wissens ist (Lang 2004, 91f).

- **Validierung dokumentierten Wissens (SO26)**: Im Hinblick auf die Ebenen der Informationsqualität können durch Maßnahmen zur Validierung die Genauigkeit, Aktualität, Konsistenz, Rechtzeitigkeit und Sicherheit verbessert werden und dabei insbesondere Risiken in Bezug auf eine unzureichende Vertrauenswürdigkeit vermindert werden (Eppler 2004, 332). So können im Speziellen mittels Schätzprüfverfahren die Plausibilität oder durch Konsistenzprüfungen Widersprüchlichkeiten reduziert werden (Eppler 2004, 334). Zudem kann durch das Heranziehen mehrerer Quellen und deren Vergleich die Nutzung inkorrekten Wissens reduziert werden (Coleman, Casselman 2004, 32; Eppler 2004, 334). Weiterhin können Autorenanalysen herangezogen werden, um die Nachvollziehbarkeit zu verbessern und durch den expliziten Einbezug der Reputation der Autoren die Qualität zu erhöhen. In diesem Zusammenhang kann eine Verbesserung der Wissensqualität auch dadurch erreicht werden, dass Beiträge von Autoren durch andere Mitarbeiter im Hinblick auf die Brauchbarkeit etc. bewertet werden (Nohr 2001, 6ff; Eppler 2004, 334).
- **Verortung dokumentierten Wissens (SO27)**: Neben der Validierung ist auch die Verortung dokumentierten Wissens eine geeignete Maßnahme, um Defizite in Bezug auf die Qualität zu reduzieren und so korrespondierende Risiken zu vermindern. Durch eine Verortung soll klar gestellt werden, inwieweit das dokumentierte Wissen in einem anderen Kontext anwendbar und korrekt ist. Zudem soll dessen Entstehung transparent gemacht werden und nachvollziehbar sein, wer sich für die Erstellung als verantwortlich zeichnet und somit als möglicher Ansprechpartner zur Verfügung steht. Insgesamt soll durch entsprechende Verortungsmaßnamen eine verbesserte Kontextualisierung des dokumentierten Wissens erreicht werden (Eppler 2004, 332). So kann im Speziellen die Zielgruppe, die für die Nutzung des dokumentierten Wissens seitens der Autoren vorgesehen wurde, angegeben werden. Zudem kann der Zweck ebenso wie der Entstehungskontext durch die Autoren angegeben werden und so die Nachvollziehbarkeit und Anwendbarkeit des dokumentierten Wissens verbessert werden. Darüber hinaus können Verlinkungen zu anderen Wissenselemen-

ten und eine Beschreibung der Metainformationen (z.B. Erstellungs-, Verfallsdatum, Autor, Bearbeitungsstatus) vorgenommen werden (Eppler 2004, 334)[219].

- **vertrauensbildende Maßnahmen (SO28)**: Weiterhin können Maßnahmen ergriffen werden, um das Vertrauen zwischen den Kooperationspartnern zu erhöhen. Vertrauen bezeichnet in diesem Kontext die Verhaltenserwartung, dass die Partner gegenseitig bereit sind, verletzbar zu sein bzw. Schwachstellen aufzuweisen, da sie erwarten, dass diese durch die Partner nicht opportunistisch ausgenutzt werden. Somit sind die Partner bereit, zu einem gewissen Grad Risiken einzugehen (Müller-Stewens, Osterloh 1996, 22f; Inkpen, Currall 2004, 588; Lucas 2005, 89). Weiterhin kann im Kontext von Kooperationen beim Vorliegen von Vertrauen davon ausgegangen werden, dass die Partner ihre Verpflichtungen in der Partnerschaft erfüllen (Inkpen 2000, 1027). Somit kann Kontrolle durch Vertrauen substituiert werden, wodurch die korrespondierenden Transaktionskosten der Kontrolle sinken (Woolthuis et al. 2002, 3ff; Norman 2004, 611). Dabei unterstützt Vertrauen die anderen Steuerungsmaßnahmen, ersetzt sie allerdings nicht vollständig und ist somit als komplementär anzusehen (Helm et al. 1996, 87; Nooteboom et al. 1997, 318).

  Vertrauen entwickelt sich auf der Mikroebene im Zeitablauf durch die Interaktion der Mitarbeiter (Wathne et al. 1996, 63). Demzufolge können Maßnahmen, die eine erhöhte Interaktion der Mitarbeiter zur Folge haben, zum Aufbau von Vertrauen beitragen. Als Beispiele können in diesem Zusammenhang Job Rotation oder gemeinsame Produktionsstandorte angeführt werden. Weiterhin nimmt Vertrauen mit der Zeit zu, wenn zunehmend Informationen über den, dem vertraut werden soll, vorliegen (Ford 2001, 556). Daher tragen Transparenz und Offenheit der Partner zum Aufbau von Vertrauen bei. Weiterhin wirken sich unterschiedliche Machtverhältnisse negativ auf das Vertrauen zwischen den Partnern aus. Aus diesem Grund kann auch eine partizipative Entscheidungsfindung positiv zum Aufbau von Vertrauen beitragen, da so hemmende Machtunterschiede kompensiert werden können (Das 2005, 714).

  Im Zusammenhang mit der Wissensqualität können ebenfalls vertrauensbildende Maßnahmen zu einer Reduktion der korrespondierenden Wissensrisiken beitragen. So kann das Vertrauen in Informationsdienste durch die Bereitstellung vollständiger, verlässlicher und glaubwürdiger Inhalte sowie die Sicherheit im Umgang mit den persönlichen Daten gefördert werden (Rittberger 2004, 162; Stock 2004, 20).

[219] Eppler unterteilt die Maßnahmen zur Verbesserung der Wissensqualität in die vier Kategorien Validierung, Verortung, Integration und Aktivierung. Von diesen vier Gruppen sind für den Untersuchungsgegenstand insbesondere die beiden erstgenannten von Relevanz. Für Details siehe (Eppler 2003c, 82ff).

5.10.3 Technische Steuerungsmaßnahmen

Nach der Darlegung der organisatorischen Steuerungsmaßnahmen, hat nachfolgender Abschnitt die Erörterung von technischen Steuerungsmaßnahmen und deren Beitrag zur Verminderung oder Vermeidung der in den Abschnitten 5.3-5.6 beschriebenen Wissensrisiken zum Gegenstand.

- **Sicherung der IT-Systeme (ST1)**: Wie bereits in Abschnitt 5.10.1 erwähnt, stellen Sicherheitsmaßnahmen in Bezug auf IT-Systeme eine Voraussetzung für die Steuerung von Wissensrisiken dar. Diese umfassen beispielsweise die Konfiguration von Firewalls, die laufende Aktualisierung von Virenscannersoftware oder die Definition von Notfallplänen (Manthei, Schmidt 2005, 79f). Ferner können Penetrationstests etc. eingesetzt werden, um festzustellen wie sicher IT-Systeme gegen externe Angriffe sind, wo Schwachstellen bestehen und wie diese behoben werden können. An dieser Stelle wird auf die einschlägigen Standards in diesem Bereich wie IT-Grundschutzkataloge, ISO 17799, CobiT etc. verwiesen (siehe hierzu auch Abschnitt 4.4).
- **Wartung der IT-Systeme (ST2):** Zusätzlich stellt auch die Wartung und Instandhaltung der IT-Systeme allgemein und der Sicherheitssysteme im Speziellen eine bedeutende Steuerungsmaßnahme dar. Von diesem Aufgabenspektrum sind u.a. die Administratoren der IT-Systeme in Bezug auf die unterbrechungsfreie und sichere Bereitstellung der Systeme und Inhalte, die Brandschutzbeauftragten in Bezug auf entsprechende Meldeanlagen oder die Haustechniker im Hinblick auf Zutrittskontrollsysteme und Einbruchsschutz betroffen (BSI 2006, 35ff). So kann in regelmäßigen Abständen bzw. nach Ablauf einer bestimmten Betriebsdauer ein Austausch von Geräten bzw. Komponenten erfolgen, um die Risikopotentiale zu senken[220].
- **Datensicherungskonzept (ST3)**: Eine zentrale Basisvoraussetzung für die Reduktion des Erwartungswertes von Wissensverlusten ist in einem leistungsfähigen Datensicherungskonzept zu sehen, das sowohl organisatorische als auch technische Aspekte einschließt. Primär organisatorische Gegenstände stellen dabei Verpflichtungserklärungen und Richtlinien für die Mitarbeiter (z.B. ausschließliche Nutzung von Netzlaufwerken) sowie die Bestimmung der zu sichernden Daten einschließlich Spezifizierung der Anforderungen im Hinblick auf Integrität und Vertraulichkeit sowie die Definition der Sicherungsart und -zyklen dar. Aus einer technischen Perspektive sind u.a. die einzubeziehenden Netzlaufwerke, die Speichermedien, die Planung der Speicherkapazitäten sowie die Lagerung von Backup-Medien relevante Fragestellungen (Mundy, Chadwick 2004, 331f; BSI 2006, 902, 3414ff)[221].
- **Einsatz von Verschlüsselungsverfahren (ST4)**: Verschlüsselung von Inhalten verhindert die Kenntnisnahme durch unautorisierte Dritte bzw. erschwert diese und eignet sich folglich primär zu einer Reduktion des Risikopotentials im Bereich der unerwünschten Diffusion. Mittels Verschlüs-

[220] Für weitere Details siehe (IT-Governance-Institute 2005; Peltier 2005; BSI 2006; Eckert 2006).
[221] Für weitere Details siehe (Cougias 2003).

selung wird eine im Klartext vorliegende Information unter Zugrundelegung eines bestimmten Verfahrens[222] und Verwendung eines Schlüssels in eine scheinbar sinnlose Zeichenfolge umgewandelt. Diese Zeichenfolge kann durch Anwendung des entsprechenden Schlüssels wiederum in Klartext umgewandelt werden (Hansen, Neumann 2005, 292).

So können im Rahmen der Kommunikation E-Mails verschlüsselt werden und so das Abhören des Datenverkehrs ver- bzw. behindert werden (BSI 2006, 1304ff). Ferner kann eine Verschlüsselung von Daten auf Festplatten vorgenommen werden, um eine Diffusion sensitiver Inhalte, die durch Einbruchdiebstähle oder den Diebstahl oder Verlust von mobilen Endgeräten ausgeht, zu begrenzen (Kruth 2004, 149). Insbesondere die Verschlüsselung von Festplatten von mobilen Endgeräten und Datenspeichern (z.B. USB-Sticks) sind relevant, da sie ein erhöhtes Risikopotential aufweisen[223].

- **Zugriffskontrollen (ST5)**: Um den unautorisierten Zugriff auf sensitive Inhalte in IT-Systemen zu verhindern, ist eine leistungsfähige Zugriffskontrolle bedeutend. Diese basiert auf der zugrunde gelegten Strategie, die in Bezug auf die definierte Vertrauensdomäne[224] variiert. So kann die Zugriffskontrolle primär unternehmensextern oder in unterschiedlichen Abstufungen auch zusätzlich unternehmensintern ausgerichtet sein (Stiemerling et al. 2000, 319; Schmidt 2006, 87f). Ferner kann die Zugriffskontrolle z.B. rollenbasiert erfolgen (Role Based Access Control, kurz: RBAC), der Eigenverantwortung des Eigentümers überlassen bleiben (Discretionary Access Control, kurz: DAC) oder auf der Vergabe von Stati für Objekte und Nutzer (z.B. geheim, vertraulich) basieren (Mandatory Access Control, kurz: MAC) (Mundy, Chadwick 2004, 327; Hansen, Neumann 2005, 310ff).

  Neben der unterschiedlich rigiden Vergabe der Zugriffsrechte auf der Basis der Strategie ist in diesem Kontext auch die Definition von Richtlinien von Relevanz, die ein Umgehen der zugewiesenen Stati absichern sollen. Diese können beispielsweise Anforderungen an die Definition, Weitergabe und Aktualisierung von Passwörtern, die Begrenzung von Administratorenrechten oder die Limitierung der Anmeldeversuche und eine entsprechende Protokollierung betreffen (Verfassungsschutz 2004a, 19). Aus technischer Perspektive ist primär die leistungsfähige Umsetzung des Zugriffskontrollkonzeptes unter Sicherheitsaspekten von Bedeutung. Dabei kann ein Ziel auch darin bestehen, die Fehleranfälligkeit bzw. das Umgehen der Zugriffskontrollen, die vielfach durch menschliches Fehlverhalten verursacht wird, zu reduzieren. In diesem Kontext kann der

[222] Zur Verschlüsselung können symmetrische und asymmetrische Verschlüsselungsverfahren herangezogen werden, wobei bei ersterem zur Ver- und Entschlüsselung identische Schlüssel genutzt werden, während bei der vergleichsweise sichereren asymmetrischen Verschlüsselung ein Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht, eingesetzt wird. Beispiele für Verfahren sind DES, IDEA, STEALTH. Für Details siehe (Hansen, Neumann 2005, 292ff).

[223] Für Details siehe z.B. (Pohlmann 2006, 31).

[224] Siehe hierzu auch Abschnitt 4.3.

Einsatz von Systemen zum Management von Identitäten (Identity Management) einen Beitrag leisten. Unter Identity Management werden Konzepte, Prozesse und Systeme zur (teil-) automatisierten Erfassung und Verwaltung von Identitäten (z.B. Benutzer von IT-Anwendungen) und zur automatisierten Kontrolle der Nutzung von Unternehmensressourcen subsumiert (z.B. IT-Anwendungen, Dokumente) (Hansen et al. 2003, 551; Rogulla, Walther 2003b, 13; De Clercq, Rouault 2004, 2; Fumy, Sauerbrey 2005, 289; Kuppinger 2005, 1; Petralia 2005, 9). So soll die Zugriffskontrolle beispielsweise durch eine zentrale Verwaltung von Identitäten im Zuge eines Single Sign-On, also einer einmaligen Authentifizierung, erleichtert und sicherer gestaltet werden[225]. Zudem sind Fragestellungen in Bezug auf eine sichere Authentifizierung z.B. durch den Einsatz biometrischer Verfahren Gegenstand der technischen Umsetzung (Mundy, Chadwick 2004, 324; Hansen, Neumann 2005, 91f). Das Management digitaler Identitäten hat auch die laufende Anpassung der Berechtigungen, die auch als Provisioning bezeichnet wird, zum Gegenstand. Provisioning umfasst dabei allgemein das Bereitstellen von Benutzern, die Festlegung von Berechtigungen für den Zugriff auf Daten, Anwendungen und Dienste sowie die Bereitstellung von anderen Ressourcen wie Rechnerzeit (IT-Research 2003, 8). Neben der Bereitstellung kommt allerdings auch der Anpassung und insbesondere auch der Löschung von Berechtigungen und Nutzern, die auch als Deprovisioning bezeichnet wird, eine besondere Bedeutung zu, um Statuswechseln, die sich aus organisatorischen Ereignissen, wie z.B. Kündigung eines Mitarbeiters, ergeben, zeitnah zu berücksichtigen (Rogulla, Walther 2003a, 21; Herwig, Schlabitz 2004, 291; Hommel, Reiser 2005, 65). Alternativ können Zugriffsrechte bei längerer Abwesenheit (z.B. Krankheit oder Urlaub) einer Person vorübergehend gesperrt werden, um Missbrauch zu verhindern (BSI 2006, 939). Die Überprüfung und Aktualisierung der Zugriffsrechte kann dabei sowohl ereignisbezogen oder in regelmäßigen Zeitabständen erfolgen.

- **Zutrittskontrollen (ST6)**: Eine weitere Reduktion des Risikopotentials in Bezug auf eine unerwünschte Diffusion oder den Verlust von wissensbezogenen Ressourcen kann durch den Einsatz von Zutrittskontrollen erreicht werden. Diese sollen gewährleisten, dass nur autorisierte Personen Zutritt zum Unternehmensgelände allgemein oder spezifischen Teilen, wie z.B. Abteilungen,[226] haben. Eine derartige Begrenzung kann auf externe Personen, wie z.B. Besucher, Mitarbeiter von Fremdfirmen, externe Dienstleister oder Mitarbeiter von Partnerunternehmen, bezogen sein. Da-

[225] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, haben 16% der beteiligten Unternehmen Identity Management Lösungen vollständig implementiert, bei 29% der Befragten besteht noch weiterer Handlungsbedarf, während 28% der befragten IT-Manager zukünftigen Handlungsbedarf sehen und 26% kein Interesse haben. In Bezug auf Single Sign-On oder fortgeschrittene Authentifizierung ist eine vollständige Implementierung in 33% erfolgt. Bei 32% der befragten IT-Manager ist dies noch nicht abgeschlossen, während 24% der Befragten in der Einrichtung von Single Sign-On Lösungen einen zukünftigen Bedarf sehen und 14% kein Interesse an einer Implementierung haben (Collins, Vile 2007, 6f).

[226] So kann beispielsweise der Zutritt zu zentralen technischen Verteilerräumen gesichert sein (BSI 2006, 829) oder durch eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern verhindert werden, dass Wartungstechniker unerlaubt auf Datenträger zugreifen (BSI 2006, 938).

rüber hinaus können sich derartige Restriktionen auch auf unternehmensinterne Mitarbeiter beziehen und beispielsweise der Zutritt zu Forschungseinrichtungen o.ä. nur einer ausgewählten Anzahl an Mitarbeitern möglich sein (Fleischer 1997, 237; Liebeskind 1997, 632f; Norman 2001, 52ff). Im Speziellen kann die Zutrittsregelung auch Drucker, Kopierer und Faxgeräte betreffen, um sicherzustellen, dass nur autorisierte Personen Kenntnis von den übermittelten Inhalten nehmen können (BSI 2006, 866, 872)[227]. Die Kontrollen können dabei auf verschiedene Art und Weise implementiert werden. So kann diese einerseits durch bauliche und technische Maßnahmen, wie z.B. Zäune, abgeschlossene Tore, Türen und Schleusen, die spezifische Sicherheitszonen im Unternehmen abgrenzen, kontrolliert werden und dabei die Authentifizierung der Personen durch technische Einrichtungen wie Chipkartenleser oder Lesegeräte für biometrische Merkmale unterstützt werden. Aus organisatorischer Sicht kann die Durchsetzung der Kontrollen durch die Identifikation von Personen durch Wach- oder Rezeptionsdienste, eine zentrale Schlüsselverwaltung oder die Begleitung externer Personen durch unternehmensinterne Mitarbeiter unterstützt werden (Maier 1992, 104ff; Dreger 1998, 317, 329; Mundy, Chadwick 2004, 324; Verfassungsschutz 2004b, 13; BSI 2006, 952, 954). Als Sonderfall kann eine geographische Separierung bestimmter Abteilungen, wie z.B. Forschungs- und Entwicklungsabteilungen, an separate abgeschlossene Standorte vorgenommen werden (Liebeskind 1997, 650).

- **Maßnahmen zur Abwehr von Reverse Engineering (ST7):** Wie bereits in Abschnitt 2.2.4 dargestellt, nimmt die Spezifität, Komplexität, Abhängigkeit von anderem Wissen Einfluss darauf, inwiefern in Objekte expliziertes Wissen, das an Dritte diffundiert ist, angewandt werden kann (Liebeskind 1997, 626ff). Während im Falle eines erwünschten Wissenstransfers Maßnahmen, wie z.B. eine Intensivierung der Zusammenarbeit oder eine gezielte Dekontextualisierung, ergriffen werden, um die Rekontextualisierung durch den Partner zu erleichtern, können in Bezug auf die Verhinderung bzw. Erschwerung einer unerwünschten Diffusion entsprechend gegenläufige Maßnahmen ergriffen werden. So kann versucht werden, die genannten Charakteristika von Wissen im Falle von Produkten, Produktbeschreibungen oder Konzepten entsprechend zu verändern. Amelingmeyer unterscheidet dabei zwischen einem funktions- und dispositionsbedingten Implizitheitsgrad. Ersterer ist in Bezug auf ein Produkt beispielsweise dessen Herstellung oder Zusammensetzung inhärent, während ein dispositionsbedingter Implizitheitsgrad seitens des Unternehmens bewusst herbeigeführt wird (Amelingmeyer 2002, 65). Darüber hinaus können Produkte so gestaltet werden, dass sie nur unter Zerstörung wesentlicher Teile analysiert werden können oder der Nachbau aufgrund hoher Komplexität und Spezifität erschwert wird. In diesem Zusammen-

[227] In diesem Zusammenhang können auch Chipkarten eingesetzt werden, mittels derer die Druckjobs dann abgerufen werden, wenn die jeweiligen Personen, die den Druckauftrag gegeben haben, am Drucker sind. So kann verhindert werden, dass insbesondere bei längeren Wegen zum Drucker oder aufgrund anderer Verzögerungen nicht autorisierte Personen Kenntnis nehmen können.

hang stellt auch die Kombination von Produkten und Services eine Option dar, da so dem Kunden Zusatzleistungen geboten werden, zu denen der potentielle Imitator nicht imstande ist (Wildemann 2007, 39). Ferner können vertragliche Regelungen, wie z.B. Miet- oder Lizenzverträge, so angepasst werden, dass sie von den Kunden vorgenommene Reparaturen an den überlassenen Produkten untersagen, um so eine Diffusion zu verhindern (Amelingmeyer 2002, 154)[228]. Darüber hinaus wird der Erfolg der Diffusion aus der Sicht des Dritten durch dessen Fähigkeiten zur Aufnahme und Aneignung des inhärenten Wissens beeinflusst (Liebeskind 1997, 629).

- **Maßnahmen zum Abhörschutz (ST8)**: Eine weitere Gruppe an Steuerungsmaßnahmen, die primär auf die Vermeidung einer unerwünschten Diffusion ausgerichtet sind, stellen Maßnahmen zur Abwehr des Abhörens von Räumen und Telekommunikationsanlagen dar. Dabei können derartige Abwehrmaßnahmen, deren Erfolg durch leistungsfähige Zutrittskontrollen erhöht wird, auf die Sicherung von Büro- und Besprechungsräumen ebenso wie auf die Absicherung von Geräten, Leitungen, Verteilerkästen, Abzweigdosen oder drahtlosen Verbindungen ausgerichtet sein. Dies betrifft beispielsweise eine regelmäßige Überprüfung bestimmter Büroräume und Telekommunikationsgeräte, um sicherzustellen, dass keine Abhörgeräte wie Wanzen oder Richtmikrofone unautorisiert angebracht wurden (Maier 1992, 124f; Verfassungsschutz 2004a, 11f; Niedermeier, Huth 2006, 16). Im Bezug auf Telefonanlagen kann dies beispielsweise mit deren Versiegelung gewährleistet werden (Meissinger 2006, 105). Dabei zählt es zu den Sorgfaltspflichten eines Geschäftsführers, dass im Falle einer Diffusion sensitiver Inhalte ein Gutachten eines unabhängigen Sachverständigen für Lauschabwehr belegt, dass sich die Geschäftsleitung mit dem Thema Lauschabwehr auseinandergesetzt hat und somit kein fahrlässiges Verhalten vorliegt (Niedermeier, Huth 2006, 17).
- **Einsatz technischer Nutzungsbeschränkungen (ST9):** Als weiterer Regelungsbereich kann die Nutzung verschiedener technischer Geräte im Unternehmen unterbunden werden, indem entsprechende Anschlüsse, wie z.B. USB-Ports, gesperrt bzw. deaktiviert werden. Auf diese Weise kann beispielsweise die Nutzung mobiler Speicher (z.B. USB-Sticks, mobile Festplatten) unterbunden werden[229], da durch diese große Datenmengen über die Unternehmensgrenzen hinaus transferiert werden können und somit mit einem erheblichen Risikopotential einhergehen (Verfassungsschutz 2004b, 16; Desouza, Vanapalli 2005, 86f; Meissinger 2006, 108)[230].
- **Digitales Rechtemanagement (ST10):** Ansätze zum Schutz sensitiver Inhalte zielen traditionell darauf ab, eine unerwünschte Diffusion zu verhindern. Dies wird im Falle physischer Dokumente z.B. dadurch erreicht, dass durch eine entsprechende Verwahrung der Personenkreis, der zugreifen

[228] Siehe hierzu auch (Schwamborn 1994, 241).
[229] Für Details siehe (BSI 2006, 2713ff).
[230] Die genannten Geräte stellen ebenso wie Kameras technische Hilfsmittel im Sinne des § 17 II UWG dar, die zur Betriebsspionage eingesetzt werden können. Siehe hierzu auch 5.10.4.

kann, eingeschränkt wird sowie Urheberinformationen oder Vertraulichkeitskennzeichnung am Dokument angebracht werden (Dreger 1998, 364). Mit zunehmender Digitalisierung der Inhalte wird einerseits dieser Schutz erschwert und andererseits nimmt auch das Risikopotential zu, da eine vergleichsweise schnellere Verbreitung erfolgen kann. Daher ist auch insbesondere der Schutz digitaler Inhalte von besonderer Bedeutung. Dabei sind eine leistungsfähige Zugriffskontrolle (siehe ST5) und der Einsatz entsprechender Richtlinien relevant. Darüber hinaus kann eine weitere Einschränkung der Rechte bzw. der Nutzbarkeit durch die Vergabe digitaler Rechte erfolgen und so das Risikopotential weiter eingeschränkt werden. Unter digitalem Rechtemanagement wird ein umfassendes Maßnahmenbündel aus vorwiegend technischen Lösungen zur sicheren zugangs- und nutzungskontrollierten Verteilung, Abrechnung und Verwaltung von primär digitalen Inhalten verstanden. Dieses Bündel schließt auch rechtliche Maßnahmen, wie z.B. Lizenzverträge, ein. Dabei bewegt sich das digitale Rechtemanagement im Spannungsfeld, die erwünschte Nutzung zu ermöglichen und zugleich die unerwünschte Nutzung zu verhindern (Fränkl, Karpf 2004, 27; Hess et al. 2004a, 54; Upadhyaya et al. 2006, 799ff). Digitale Rechte sind dabei allerdings nicht mit Kopierschutz, der den Schutz des Datenträgers zum Inhalt hat, gleichzusetzen, sondern stellen auf den Schutz der Inhalte ab (Fränkl, Karpf 2004, 6f). Fokussiert man die technische Komponente, so sind folgende Kerntechniken für das digitale Rechtemanagement von besonderer Relevanz. So werden einerseits Verschlüsselungsverfahren und andererseits spezifische Rechtemanagement-Sprachen, wie z.B. ODRL[231] und XrML,[232] eingesetzt. Zudem stellen digitale Wasserzeichen eine Basiskomponente dar. Letztere ermöglichen die Einbettung von Metadaten insbesondere in Bezug auf Nutzungsrechte, wobei vielfach steganographische Verfahren eingesetzt werden. Wasserzeichen können allerdings nur nachträglich zur Identifikation von Urheberrechtsverletzungen herangezogen werden und dienen daher der Durchsetzung von rechtlichen Ansprüchen in Bezug auf die Urheberrechtsverletzung etc. (Cheung, Chiu 2003; Hess et al. 2004b, 12f; Hansen, Neumann 2005, 295f). Die Rechte können sich dabei auf die drei Bereiche Wiedergabe, Transport und Erstellung abgeleiteter Werke beziehen. Auf den Unternehmenseinsatz fokussiert betrifft dies das Wiedergaberecht, das Lesen einer Datei oder das Ausdrucken. So können beispielsweise Einschränkungen in Bezug auf die Anzahl der erlaubten Ausdrucke oder im Hinblick auf die gestattete Druckauflösung erfolgen. Rechte in Bezug auf den Transport beziehen sich auf das Kopieren oder die Verteilung. So kann die Nutzung an bestimmte Arbeitsplatzrechner oder Endgeräte gebunden sein, wie es z.B. vielfach bei eBooks im kommerziellen Einsatz der Fall ist. Das Recht abgeleitete Werke zu erstellen, betrifft das Kopieren, Editieren und Einfügen von Texten oder Bilder in Dokumente. Die Ausübung dieser Rechte ist in der Standardsoftware zur Textverarbeitung in-

[231] ODRL steht für Open Digital Rights Language. Für weitere Details siehe (Ianella 2002).
[232] XrML steht für eXtensible rights Markup Language. Für weitere Details siehe www.xrml.org/.

tegriert[233]. Zudem sind Ansätze in Entwicklung, mittels derer auf der Ebene von Dokumenten Berechtigungen für einzelne Passagen vergeben werden[234].

- **Sicherstellung hoher Medienqualität (ST11)**: Im Hinblick auf die Nutzung dokumentierten Wissens durch die Mitarbeiter im Rahmen wissensintensiver Aufgaben ist es entscheidend, dass durch die IT-Infrastruktur eine hohe Medienqualität gewährleistet wird. Dies betrifft beispielsweise die Verfügbarkeit, Sicherheit und Nutzbarkeit. In Bezug auf die Verfügbarkeit kann dies durch die Bereitstellung eines zweiten Systems im Standby- oder Parallelbetrieb erfolgen (BSI 2006, 1721ff), während die Sicherheit durch den Schutz der IT-Systeme gegen unautorisierte Zugriffe und Verluste gewährleistet werden kann (siehe hierzu auch ST1). Weiterhin können die Integration verschiedener Quellen, die Personalisierung der Inhalte oder eine verbesserte Visualisierung zu einer vergleichsweise höheren Nutzbarkeit beitragen (Eppler 2003c, 92ff).

5.10.4 Rechtliche Steuerungsmaßnahmen

Als dritte Kategorie werden nachfolgend rechtliche Steuerungsmaßnahmen zur Begrenzung der Wissensrisikopotentiale erörtert.

- **Geheimhaltungsvereinbarungen (SR1)**: Als Steuerungsmaßnahme, die primär auf die unerwünschte Diffusion von Wissen abstellt, kann mit den Mitarbeitern sowie mit externen Dienstleistern und Partnern Geheimhaltung vereinbart werden, deren Missachtung bei Erfüllung der entsprechenden Tatbestände gesetzliche Ansprüche ermöglicht. Geheimhaltung in Bezug auf Wissen setzt dessen Klassifikation im Hinblick auf die Vertraulichkeit des Wissens sowie eine genaue Definition der damit einhergehenden Rechte und Pflichten voraus (Marsland 2003, 166). Allgemein schreiben diese Vereinbarungen die Verschwiegenheit in Bezug auf Betriebs- und Geschäftsgeheimnisse vor. Derartigen Vereinbarungen kommt bei allen Vertragsverhältnissen eine Bedeutung zu, bei denen mindestens eine Partei Einblick in sensitive Inhalte der anderen Partei enthält (Schubert 2005, 15f). Vertragsparteien können in diesem Zusammenhang Arbeitgeber und -nehmer, Auftraggeber und -nehmer oder Partnern sein (Norman 2001, 54; Amelingmeyer 2002, 154f)[235]. Bei der Abfassung der Vereinbarung sollten die von der Geheimhaltung betroffenen Gegenstände wie z.B. Themen, Projekte oder Produkte detailliert, Ausnahmefälle definiert oder auch der Umgang mit Dokumenten geregelt werden. Generell ist es allerdings schwer zu unterscheiden, ob eine Verwertung rechtmäßig erlangter Kenntnisse oder Erfahrungen erfolgte oder ob diese die Preisgabe eines Betriebsgeheimnisses betrifft (Maier 1992, 74f, 108f; Schubert 2005, 15f). Eine

[233] So ist beispielsweise ein Passwortschutz in Microsoft Word oder in den Produkten Adobe Standard oder Professional möglich.

[234] Siehe hierzu z.B. den Ansatz Safe Docs (Nosek 2006).

[235] Nach einer aktuellen Studie zum Thema Informationsrisiken, die mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, sind bei ca. 50% der befragten Unternehmen Geheimhaltungsvereinbarungen Gegenstand von Arbeitsverträgen (Vile 2007, 4).

gesetzliche Grundlage für die Geheimhaltungsverpflichtung stellen die §§ 17-18 UWG[236] dar. Teilt nach § 17 I UWG ein Mitarbeiter des Unternehmens ein ihm anvertrautes Geschäfts- oder Betriebsgeheimnis einem Dritten zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht dem Unternehmen zu schaden mit, liegt ein gesetzlicher Verstoß vor, der eine Geldstrafe oder Freiheitsstrafe von drei Jahren[237] nach sich ziehen kann. Damit der Sachverhalt erfüllt ist, muss es sich tatsächlich um ein Geschäfts- oder Betriebsgeheimnis handeln. Dies ist nach der Rechtssprechung der Fall, wenn die Inhalte nur einem begrenzten Personenkreis bekannt ist, der Geheimhaltungswille des Inhabers erkennbar ist, ein schutzwürdiges Interesse an der Geheimhaltung besteht und die Inhalte Dritten nicht ohne weiteres zugänglich sind. Zur Erfüllung des Tatbestandes sind schriftliche Vereinbarungen erforderlich, da so Geheimhaltungswille erkennbar dokumentiert wird. Ferner muss nachgewiesen werden, dass entsprechende Schutzmaßnahmen im Sinne von Zugangs- und Zugriffskontrollen ergriffen wurden. Der Geheimnisverrat durch Beschäftigte § 17 I UWG gilt nur für die Dauer des Beschäftigungsverhältnisses. Somit kann der Wechsel zu einem Konkurrenzunternehmen und die damit verbundene Diffusion nur durch den Einsatz von zusätzlichen Konkurrenzschutzklauseln (siehe SR2) behindert werden. Für deren Wirksamkeit muss allerdings der Tatbestand erfüllt sein, dass Mitarbeiter nicht erheblich in ihrer beruflichen Entwicklung eingeschränkt werden (Schubert 2005, 2ff). § 17 II UWG regelt die Betriebsspionage bzw. die Geheimnishehlerei und stellt gesetzliche Ansprüche an diejenigen unternehmensinternen und -externen Personen, die einen Nutzen aus der Verwertung ziehen. Nach § 18 UWG ist auch die eigennützige oder wettbewerbsbezogene Verwertung von anvertrauten Vorlagen, wie z.B. Zeichnungen, Modelle oder Rezepte, ein Straftatbestand, der eine Geld- oder Freiheitsstrafe von bis zu zwei Jahren nach sich ziehen kann. Nach § 19 UWG ist auch das eigennützige bzw. wettbewerbsbezogene Anstiften bzw. Verleiten zu einer Straftat, die die Tatbestände der §§ 17 oder 18 UWG erfüllt, strafbar und kann ebenfalls eine Geld- oder Freiheitsstrafe von bis zu zwei Jahren nach sich ziehen. Zivilrechtliche Ansprüche betreffen Abwehr und Unterlassung (z.B. Verbot der Nutzung), Beseitigung, Auskunft und Schadensersatz (Schubert 2005, 6)[238].

[236] UWG steht für Gesetz gegen unlauteren Wettbewerb.

[237] In besonders schweren Fällen beträgt die Freiheitsstrafe nach § 17 IV UWG bis zu fünf Jahren.

[238] Weitere gesetzliche Verankerungen einer Verpflichtung zur Geheimhaltung sind in zahlreichen weiteren Gesetzen zu finden. So wird im Aktiengesetz §§ 395 und 404 AktG die Verschwiegenheit im Falle der Beteiligung einer Gebietskörperschaft in § 395 AktG vorgeschrieben. Zudem wird die Verletzung der Verschwiegenheit durch Mitglieder des Vorstands, des Aufsichtsrats, Abwickler, Prüfer oder Gehilfen eines Prüfers in § 404 AktG geregelt und kann eine Geld- oder Freiheitsstrafe von bis zu drei Jahren nach sich ziehen. In § 85 GmbHG besteht eine analoge Vorschrift die Weitergabe von Geschäfts- oder Betriebsgeheimnissen durch Geschäftsführer, Mitglieder des Aufsichtsrats oder Liquidatoren, die als Rechtsfolge eine Geld- oder Freiheitsstrafe von bis zu drei Jahren nach sich ziehen kann. Eine analoge Verpflichtung, die Erwerbs- und Wirtschaftsgenossenschaften betrifft und im Vergleich zu den zuvor genannten Personen auch Prüfer und deren Gehilfen einschließt und abweichend eine Freiheitsstrafe von bis zu einem Jahr nach sich ziehen kann, besteht in § 151 GenG. Im Handelsgesetzbuch besteht in § 90 HGB eine Verpflichtung von Handelsvertretern zur Geheimhaltung von anvertrauten Geschäfts- und Betriebsgeheimnissen, die auch eine Verwertung bzw. Weitergabe nach Beendigung des Vertragsverhältnisses einschließt. Nach § 333 HGB werden Abschlussprüfer und de-

Die Durchsetzbarkeit dieser gesetzlichen Rechtsfolgen hängt davon ab, inwiefern seitens des Unternehmens nachgewiesen werden kann, dass es sich tatsächlich um ein Betriebs- bzw. Geschäftsgeheimnis handelt und entsprechende Schutzmaßnahmen ergriffen wurden. Somit steht diese rechtliche Maßnahme in starker Interaktion mit anderen Steuerungsmaßnahmen, die auf die Vermeidung einer unerwünschten Diffusion fokussiert sind.

- **Konkurrenzschutzklauseln (SR2):** Um eine unerwünschte Diffusion von Wissen an Konkurrenten und somit eine potentielle Verzerrung von Wettbewerbsvorteilen zu verhindern bzw. zu erschweren, können Konkurrenzschutzklauseln als Bestandteil von Arbeitsverträgen oder als Zusatzvereinbarung abgeschlossen werden. Diese Klauseln haben zum Ziel, Mitarbeitern für einen bestimmten Zeitraum zu verbieten ‚für Konkurrenten zu arbeiten und haben somit die Intention die Anwendung von unternehmensspezifischem Wissen bei Konkurrenten für einen bestimmten Zeitraum zu verhindern (Maier 1992, 76f; Liebeskind 1997, 634; Rønde 2001, 406). Dabei kann gemäß der gesetzlichen Grundlage des § 74 HGB dem Arbeitnehmer für maximal einen Zeitraum von zwei Jahren den Wechsel zu einem Konkurrenten oder den Wechsel in die Selbständigkeit verboten werden. Für die Dauer des Wettbewerbsverbotes ist nach § 74 II HGB dem Arbeitnehmer eine Karenzentschädigung zu entrichten ist. Gemäß § 74a II HGB wird der Geltungsbereich des Wettbewerbsverbotes allerdings dahingehend begrenzt, dass der Mitarbeiter in seinem beruflichen Fortkommen nicht gehindert werden darf. Somit besteht ein primäres Problem der Konkurrenzschutzklauseln darin, dass ihre Durchsetzbarkeit in der Praxis schwer ist, da sie Gerichte oftmals mit der Begründung nicht anerkennen, dass Mitarbeiter bei der Wahl des Arbeitgebers nicht eingeschränkt werden dürfen.
- **Kooperationsvereinbarungen (SR3):** Eine weitere Steuerungsmaßnahme mit rechtlicher Durchsetzbarkeit stellen Kooperationsvereinbarungen dar, die über Geheimhaltungsvereinbarungen hinausgehend den Umgang mit Wissen, das im Rahmen der Kooperation generiert bzw. ausgetauscht wurde, regeln. Derartige Vereinbarungen können formlos getroffen werden, sind aber vielfach vertraglich fixiert und stellen somit eine präventive absichernde Maßnahme dar (Sell 1994,

ren Gehilfen ebenfalls zur Geheimhaltung verpflichtet und bei Nichteinhaltung mit einer Geld- oder Freiheitsstrafe von bis zu einem Jahr belangt. Im Betriebsverfassungsgesetz wird in § 120 BetrVG die Geheimhaltungsverpflichtung für (Ersatz-)Mitglieder des Betriebsrats, Vertreter einer Gewerkschaft oder Arbeitgebervereinigung, Sachverständige, Berater, Auskunftspersonen und Arbeitnehmer geregelt, die neben einer Geld- auch eine Freiheitsstrafe von bis zu einem Jahr zur Folge haben kann. Letztlich bestehen entsprechende Regelungen auch im Strafgesetzbuch. So regelt § 203 StGB die Verletzung Betriebs- und Geschäftsgeheimnissen, das z.B. bedingt durch die Tätigkeit als Arzt, Rechtsanwalt, Patentanwalt, Mitarbeiter einer Krankenkasse oder Versicherung anvertraut wurde, mit Geld- und Freiheitsstrafen von bis zu einem Jahr als Rechtsfolge. § 204 StGB regelt die Verwertung des Geheimnisses, die abweichend eine Freiheitsstrafe bis zu zwei Jahren nach sich ziehen kann. Ferner wird in § 353b StGB die Verletzung eines Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht, die Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen, besteht geregelt und kann Gels- und Freiheitsstrafen bis zu 5 Jahren nach sich ziehen.

15f; Liebeskind 1997, 632; Das 2005, 708)[239]. Demnach können Kooperationsvereinbarungen dazu dienen, Probleme und Risiken im Kooperationsverlauf oder bei ihrer Auflösung zu vermeiden. Speziell in Bezug auf Wissen können diese Vereinbarungen regeln, welches Wissen Gegenstand der Kooperation ist, wie Geheimhaltung sicherzustellen ist, inwiefern eine Nutzung außerhalb der Kooperation erfolgen kann und wie bei der Auflösung der Kooperation z.B. im Hinblick auf ein Wettbewerbsverbot zu verfahren ist (Loebbecke et al. 1999, 20; Norman 2001, 52ff; Schubert 2005, 16f). Dabei sind insbesondere auch Regelungen zur Weitergabe bzw. zur Geheimhaltung vor Dritten bedeutend, da über mehrstufige Transferprozesse sensitive Inhalte in den Kenntnisbereich von direkten Konkurrenten gelangen können und so erhebliche wettbewerbsrelevante Auswirkungen nach sich ziehen können (Erickson, Rothberg 2005, 11). Darüber hinaus können auch explizit Vertragsstrafen, die über die gesetzlichen Ansprüche hinausgehen, vereinbart werden, um die Abschreckungswirkung der Vereinbarungen zu erhöhen.

- **vertragliche Regelungen für externe Dienstleister (SR4)**: Die Überlassung von sensitiven Inhalten und die Bereitstellung von Systemen durch externe Dienstleister bzw. Outsourcinganbieter erfordern vertragliche Vereinbarungen, um einerseits die Wahrung der Vertraulichkeit der überlassenen Inhalte zu sichern und somit eine unerwünschte Diffusion zu verhindern. Andererseits sind bei der Bereitstellung von Systemen und der von diesen verwalteten Inhalten durch den Outsourcinganbieter auch deren Verfügbarkeit, Fehlerbehebungszeiten bzw. Schutz gegen Verlust zu gewährleisten, um so einer Hemmung der erwünschten Prozesse entgegenzuwirken (Riedl 2003, 9; Schomann, Bloech 2005, 236). Somit können bei der Auswahl eines Outsourcing-Partners bestimmte Anforderungen an die Sicherheit gestellt werden. So kann beispielsweise eingefordert werden, dass der Outsourcing-Dienstleister über ein IT-Sicherheitskonzept verfügt und dieses umsetzt. Darüber hinaus können spezifische Anforderungen für die einzelnen Schnittstellen definiert werden. Zudem ist eine Determinierung des Schutzbedarfes der überlassenen Inhalte im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit zu definieren. Zudem können Anforderungen bezüglich des Einsatzes zertifizierter Produkte (z.B. nach Common Criteria[240]) ebenso wie die Verschlüsselung der Kommunikation oder des Datenverkehrs definiert werden (BSI 2006, 1574ff). Darüber hinaus kann bereits bei der Auswahl eines Outsourcinganbieters darauf geachtet werden, dass der Partner über Zertifizierungen im Bereich IT-Sicherheit (z.B. ISO 17799) verfügt, da eine vorhandene Zertifizierung signalisiert, dass entsprechende Normen eingehalten werden, ein gewisses Maß an Sicherheit besteht und die erfolgreiche Kontrolle durch eine unabhängige Instanz erfolgte (Krcmar, Junginger 2003, 259f). Neben der Beachtung von Zertifizierungen können sowohl vor als auch nach Vertragsabschluss Kontrollen im Hinblick auf die Eignung des Partners

[239] Details zu den Gegenständen einer umfassenden Kooperationsvereinbarung sind bei (Staudt 1992, 145ff) zu finden.
[240] Siehe hierzu Abschnitt 4.4.3.

bzw. in Bezug auf die Einhaltung der Anforderungen durchgeführt werden. Für eine zusätzliche Absicherung können Inhalte, die eine zu hohe Sensitivität aufweisen z.B. durch Verschlüsselungsverfahren geschützt werden (Fitzgerald 2004).

- **Abwehr von Betriebsspionage /-sabotage (SR5)**: Neben rechtlichen Ansprüchen in Bezug auf die Verletzung von Geheimhaltungsvereinbarungen (siehe SR1) durch Mitarbeiter, Partner, Auftragnehmer, Prüfer oder sonstige Personen, denen entsprechende Geheimnisse geschäftsbedingt offenbart werden, können Ansprüche auch gegenüber sonstigen Dritten geltend gemacht werden, die sich unberechtigt Kenntnis verschafft haben. So regelt § 17 II Nr.2 UWG auch den Fall, dass sich Dritte, wie z.B. Hacker, Spione oder Diebe, Kenntnis über Betriebsgeheimnisse verschaffen und diese unbefugt verwerten oder weitergeben. Zur Erfüllung des Tatbestandes ist es dabei erforderlich, dass technische Mittel, wie z.B. Kopierer, Scanner, Fotokameras, Wanzen oder das Eindringen in fremde Computernetze, eingesetzt wurden, was im Umkehrschluss allerdings auch bedeutet, dass sämtliche Fälle, in denen eine Kenntnisnahme ohne technische Hilfsmittel, also nur mit den Sinnen, erfolgt, ausgeschlossen werden. Somit bewegt sich das Risiko Aushorchung z.B. im Rahmen von Social Engineering Versuchen (siehe DE1) im juristischen Graubereich und erfüllt den Tatbestand des § 17 II UWG nicht (Schubert 2005, 4f). Die Rechtsfolgen sind analog zu Verletzungen bei Geheimhaltungsvereinbarungen und betreffen zivilrechtliche Ansprüche in den §§ 17 und 18 UWG, die Geld- oder Freiheitsstrafen von bis zu fünf Jahren nach sich ziehen können[241]. Die Schnittstelle zur organisatorischen Durchsetzung der Abwehr von Betriebsspionage besteht in Bezug auf Zugriffs- und Zutrittskontrollen sowie die Implementierung entsprechender Richtlinien bzgl. des Verhaltens der Mitarbeiter. In sicherheitsrelevanten Branchen bzw. im militärischen Bereich werden eigene Teams zur Abwehr derartiger Spionage eingesetzt (Desouza, Vanapalli 2005, 82f).

[241] Auch strafrechtlich kann Betriebsspionage, die eine Verletzung des Briefgeheimnisses (§ 202 StGB) oder das Ausspähen von Daten (§ 202a StGB) betrifft, verfolgt werden. So besteht nach § 202 StGB ein Straftatbestand, der eine Geld- oder Freiheitsstrafe von bis zu einem Jahr zur Folge haben kann, darin, einen Brief oder einen entsprechend verschlossenen Umschlag zu öffnen und vom Inhalt Kenntnis zu nehmen. Das Ausspähen von Daten, die gegen unberechtigten Zugang besonders gesichert sind, stellt nach § 202a StGB einen Straftatbestand dar, der auf computergespeicherte Daten beschränkt ist und somit schriftlich fixierte oder andere unmittelbar wahrnehmbaren Daten ausschließt. Wie auch im Falle der Verletzung der Geheimhaltungsverpflichtung (siehe SR1 sowie § 17 UWG) muss der Geschädigte nachweisen, dass die Daten entsprechend z.B. durch den Einsatz von Zugriffskontrollen gesichert waren, wobei nicht die Leistungsfähigkeit der Schutzmaßnahmen, sondern vielmehr der erkennbare Geheimhaltungswille ausschlaggebend ist. Zudem muss der Tatbestand des „Sich-Verschaffen“ erfüllt sein. Dies bedeutet, dass eine bewusste Aufnahme bzw. eine Speicherung der Daten seitens des Täters erforderlich ist. Die Erfüllung der Tatbestände wird mit Freiheitsstrafe bis zu drei Jahren oder mit einer Geldstrafe geahndet. Neben der Kenntnisnahme und Verwertung geschützter Daten ist auch deren Veränderung ein Straftatbestand, der sich an § 202a StGB anschließt und in § 303a StGB geregelt ist. Demnach ist es strafbar, rechtswidrig erlangte Daten nach § 202a StGB zu löschen, unbrauchbar zu machen oder zu verändern. Dies kann beispielsweise durch Verfälschen von Datensätzen, Einschleusung von Schadsoftware oder Einsetzen einer Programmsperre erfolgen. Ist das Ausmaß der Schädigung so erheblich, dass die Datenverarbeitung gestört ist, ist der Straftatbestand der Computersabotage nach § 303b StGB erfüllt, der eine Geldstrafe und eine Freiheitsstrafe von bis zu fünf Jahren nach sich ziehen kann (Schubert 2005, 7f).

- **gewerbliche Schutzrechte (SR6)**: Eine weitere Steuerungsmöglichkeit ist im Einsatz von gewerblichen Schutzrechten bzw. Intellectual Property Rights zu sehen. Deren primäres Ziel besteht darin, durch die Einschränkung der Nutzbarkeit bzw. das explizite Verbot der Nutzung einer Entwertung von Wissen entgegenzuwirken. Unter dem Begriff wird eine Vielzahl verschiedener Schutzrechte wie Patente, Marken, Sorten, Geschmacks-, Gebrauchsmuster oder Urheberrechte subsumiert, wobei nachfolgend die für den Untersuchungsgegenstand Wissensrisiko relevanten Aspekte herangezogen werden. Das Patent ist ein Schutzrecht, das nach § 1 PatG[242] für Erfindungen, die neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind, erteilt wird. Dabei kann feiner zwischen Erzeugnisschutz (z.B. Maschinen, chemische oder pharmazeutische Substanzen) und Verfahrensschutz (z.B. Herstellungsverfahren) unterschieden werden. Zentrale Voraussetzung ist dabei, dass die Problemlösung für technische Sachverhalte neuartig ist, d.h. nicht Stand der Technik ist (§ 3 PatG)[243]. Die Problemlösung muss zudem als erfinderisch eingestuft werden und darf für einen Fachmann mit durchschnittlichen Kenntnissen nicht nahe liegend sein (§ 4 PatG). Als weitere Voraussetzung muss die Erfindung gewerblich anwendbar sein (§ 5 PatG). Insbesondere zur Gewährleistung der beiden erst genannten Anforderungen wird eine inhaltliche Überprüfung des Patentantrags durch jeweilige Fachgebietsspezialisten vorgenommen und folglich ein Patent auch als geprüftes Schutzrecht bezeichnet. Nach § 16 PatG gilt ein Patent maximal 20 Jahre ab dem Tag, an dem es angemeldet wurde. Für diesen Zeitraum wird nach § 9 PatG dem Patentinhaber ein Ausschließlichkeitsrecht zur Nutzung der Erfindung eingeräumt. Zu dieser besteht auch ein entsprechender Unterlassungsanspruch nach § 139 I PatG. Neben Unterlassung besteht nach § 139 II PatG bei einer verschuldeten Verletzung des Ausschließlichkeitsrechts auch ein Schadensersatzanspruch. Bei fehlendem Verschulden können Ansprüche in Bezug auf die ungerechtfertigte Bereicherung nach § 812 BGB geltend gemacht werden. Die Dauer der Prüfung durch das Patentamt beträgt mindestens 18 Monaten, wobei nach ca. acht Monaten ein erster sachlicher Bescheid zugeteilt wird. Die Erfindung selbst wird 18 Monate nach der Patentanmeldung offen gelegt und ist somit allgemein zugänglich[244]. Die Offenlegung unterbleibt, wenn der Anmelder den Patentantrag zurückzieht. Vor Patenterteilung besteht nach § 33 PatG ein Anspruch auf Entschädigung. Wird der Antrag zurückgezogen oder das Patent nach Prüfung nicht erteilt, gilt der Anspruch auf Entschädigung jedoch nach § 58 II PatG als von Anfang an nicht eingetreten. Dabei können diese Rechte auch verkauft, lizenziert oder vererbt werden (Lehmann 2002, 11; Schubert 2005, 17).

  Ein weiteres Schutzrecht stellen Gebrauchsmuster dar, die auch als „kleines Patent“ bezeichnet

[242] Die nachfolgenden Ausführungen basieren primär auf dem Patentgesetz (PatG)

[243] Diejenigen Kenntnisse, die schriftlich, mündlich oder praktisch öffentlich geworden sind, werden als zum Stand der Technik gehörend angesehen.

[244] Angemeldete Patente können beispielsweise über im Deutschen Patent- und Markenamt (www.depatisnet.dpma.de) oder im Europäischen Patentamt (www.ep.espacenet.com) eingesehen werden.

werden, allerdings einen Verfahrensschutz ausschließen (§ 2 GebrMG). Gebrauchsmuster betreffen dieselben Gegenstände wie Patente (§ 1 GebrMG), werden aber bereits wenige Wochen bis Monate nach dem Anmeldetag eingetragen. Im Gegensatz zum Patent wird die Anmeldung allerdings nur auf formelle Richtigkeit geprüft und nicht darauf, ob der Gegenstand tatsächlich schutzwürdig ist. Eine Gebrauchsmusteranmeldung ist im Vergleich zu Patentanmeldung schneller und kann nach etwa drei Monaten mit der Eintragung in das Gebrauchsmusterregister abgeschlossen sein (Lehmann 2002, 16)[245]. In dieser Hinsicht weisen Geschmacksmuster einen eindeutigen Vorteil gegenüber Patenten auf (Wildemann 2007, 40). Im Urhebergesetz sind weitere Schutzrechte verankert, die dem Urheber eines literarischen, wissenschaftlichen oder künstlerischen Werkes rechtliche Ansprüche gewähren (§ 1 UrhG). Damit der Tatbestand eines geschützten Werkes vorliegt, muss es sich um eine geistige Schöpfung handeln, die eine gewisse Kreativität erfordert (§ 2 UrhG).

Im Unterschied zu Patenten und Gebrauchsmustern bestehen diese Rechte ohne Anmelde- und Prüfverfahren. Das Recht zur Verwertung des Werkes steht dabei dem Urheber selbst zu. Dieser kann entscheiden, inwiefern das Werk in körperlicher Form vervielfältigt, verbreitet, ausgestellt, bearbeitet oder im Falle einer unkörperlichen Form wiedergegeben werden darf (§§ 15ff UrhG). Nach § 97 I UrhG besteht ein Unterlassungsanspruch, der das Vorliegen einer Urheberrechtsverletzung und eine Wiederholungsgefahr als Tatbestandsmerkmale voraussetzt. Im Falle von Verschulden im Sinne von Fahrlässigkeit oder Vorsatz besteht zudem nach § 97 I UrhG ein Anspruch auf Schadensersatz. Dabei ist der Schaden vielfach schwer quantifizierbar. In diesem Fall behilft sich die Rechtsprechung zum Teil mit der Lizenzanalogie, nach der im Zweifel als Schaden der Betrag anzusetzen, den der Geschädigte bei einer ordnungsgemäßen Lizenzierung erzielen hätte können. Gemäß § 98 UrhG hat der Urheber auch einen Anspruch auf Vernichtung oder Überlassung der Vervielfältigungsstücke. Weitere strafrechtliche Rechtsfolgen zu Urheberrechtsverletzungen sind Gegenstand der §§ 106ff UrhG. In § 106 UrhG wird die unberechtigte Verwertung von Werken geregelt, die Geldstrafen oder Freiheitsstrafen von bis zu drei Jahren nach sich ziehen kann[246].

Generell besteht bei gewerblichen Schutzrechten ein Durchsetzbarkeitsproblem im internationalen Kontext, da zwar internationale Vereinbarungen, wie z.B. das TRIPS[247] Abkommen, bestehen und auch durch eine Vielzahl an Ländern unterzeichnet sind, jedoch die Durchsetzung der Vereinba-

[245] Neben Patenten und Gebrauchsmustern sind auch Topographien von Halbleitererzeugnissen durch das Halbleiterschutzgesetz (HalblSchG), ästhetische Gestaltungen wie zwei- oder dreidimensionale Erscheinungsformen durch das Geschmacksmustergesetz (GeschmMG), Pflanzensorten durch das Sortenschutzgesetz (SoSchG) sowie Marken durch das Markengesetz (MarkenG) geschützt. Auch in diesen Fällen erfolgt eine Eintragung in das jeweilige Register.

[246] Wird ein Werk im Rahmen eines Arbeitsverhältnisses erstellt, so steht es dem Arbeitgeber zu. Dennoch sollte dies auch schriftlich in Verträgen fixiert sein, um gerichtliche Probleme zu vermeiden (Lee 2005, 158).

[247] TRIPS steht für Trade Related Aspects of Intellectual Property Rights und wurde von der World Trade Organization entwickelt.

rungen durch nationales Recht geregelt ist und somit Schwachstellen aufweist (Baughn et al. 1997, 104; Maskus 2003, 185; Fitzgerald 2004). Der Einsatz von Patenten wird zweideutig diskutiert. So schützen Patente einerseits den Urheber, indem sie das Recht einräumen, Dritte von der Anwendung oder Herstellung der Erfindung auszuschließen. Andererseits gehen Patente mit einer Veröffentlichung der Patentanmeldung 18 Monate nach Einreichung des Antrags einher. Dadurch erfolgt unter Umständen eine Offenlegung, die durch Dritte gewinnbringend genutzt werden kann, indem diese beispielsweise legal um die patentiere Erfindung herum entwickeln (Nieto, Pérez-Cano 2004, 118f). Darüber hinaus verlieren Patente aufgrund eines vielfach kurzen Produktlebenszykluses in manchen Branchen an Bedeutung. So ist es z.B. in der Pharmaindustrie oftmals nur eine Frage der Zeit, bis ein Konkurrent ein Alternativprodukt entwickelt hat. Zudem ist es insbesondere in frühen Phasen nur schwer möglich die Rechte bei Imitation geltend zu machen. Somit ist es bei Produkten mit kurzem Produktlebenszyklus zum Teil effizienter, anstelle der Patentierung auf eine Geheimhaltung zu fokussieren, da diese Produkte bedingt durch die hohe Dauer der Patentierung den meisten Umsatz generiert haben, wenn das Patent erteilt wird und zudem keine Offenlegung der Patentanmeldung erfolgt (Rønde 2001, 392; Nieto, Pérez-Cano 2004, 118f; Reitzig 2004, 36f). Insgesamt sind Schutzrechte in Bezug auf wissensbezogene Ressourcen erforderlich, um Dritte von der Nutzung auszuschließen. Jedoch wird die Durchsetzung der Schutzrechte v.a. durch die Intangibilität und Dynamik erschwert (Choi et al. 2005, 70). Ein generelles Problem von Schutzrechten, das zur Folge hat, dass deren alleiniger Einsatz nicht ausreichend ist, besteht darin, dass diese Rechte erst dann ihre Wirkung entfalten, wenn der Schaden bereits eingetreten ist (Wildemann 2007, 39). Somit können gewerbliche Schutzrechte nur als additive Maßnahme gesehen werden. Im Speziellen können Patente neben der ausschließlichen Nutzung der Erfindung darauf abzielen, Entwicklungen der Konkurrenten zu blockieren (Blind et al. 2007, 2f).

Die mit der Einreichung eines Patentes einhergehende Veröffentlichung stellt in vielfacher Hinsicht für Unternehmen ein Risiko dar, da Konkurrenten Kenntnis von der Erfindung nehmen können und diese in einem anderen Anwendungskontext einsetzen können. Besonders evident ist diese Problematik im Bereich der Softwarepatente. Dabei ist die Patentierbarkeit von Algorithmen bedingt durch die enge Auffassung des Technikbegriffs durch den Bundesgerichtshof seit langem schwer durchsetzbar. In der jüngeren Vergangenheit ist es allerdings immer häufiger zur Patentierung von Algorithmen gekommen. Bei einer erfolgreichen Patentierung wird aber aufgrund des Freihaltungsinteresses des BGH eine Eingrenzung auf einen bestimmten Anwendungsfall vorgenommen. Dies bedeutet, dass ein Algorithmus für eine spezifische Problemlösung patentiert ist, aber zugleich dessen Anwendung zur Lösung eines anderen Problems vielfach nicht ausgeschlossen wird. Somit kann der Schaden, der aus der Patentierung im Vergleich zum entgegenstehenden

Nutzen vergleichsweise höher sein und eine Patentierung für ein Unternehmen somit nicht attraktiv sein[248].

5.11 Zusammenfassung und Diskussion

In den vorangegangenen Abschnitten wurden sowohl die in der Literatur identifizierten Wissensrisiken als auch die potentiellen Steuerungsmaßnahmen diskutiert. In diesem Abschnitt erfolgt eine vernetzte Betrachtung, die aufzeigen soll, inwieweit Einzelrisiken der vier Konzepte gesteuert werden könnten. Diese Vernetzung basiert wie in den Abschnitten 5.10.2 bis 5.10.4 dargelegt zum Teil auf der Literatur, wird aber durch Plausibilitätsüberlegungen ergänzt, da zum aktuellen Stand der Forschung keine integrierte Betrachtung vorgenommen wurde.

Dennoch können durch die integrierte Betrachtung erste Anhaltspunkte gegeben werden, welche Risiken möglicherweise mehrfach steuerbar sind und in Bezug auf welche Risiken Defizite bestehen. Darüber hinaus ergeben sich Anhaltspunkte für Steuerungsmaßnahmen, durch deren Einsatz mehrere Wissensrisiken begrenzt werden können. Unterstellt man gleiche Risikoerwartungswerte lässt sich durch die Ergreifung dieser Maßnahmen die Gesamtrisikoposition vergleichsweise stärker reduzieren. Somit kann die Analyse der Mehrfachsteuerung die Allokation der Steuerungsmaßnahmen unterstützen.

In Tab. 14 ist zusammengefasst, welche Risiken durch die in den Abschnitten 5.10.2-5.10.4 dargestellten Maßnahmen gesteuert werden können, wobei Maßnahmen, die potentiell mehrere Wissensrisiken steuern hervorgehoben werden.

So könnten durch Richtlinien zur Meldung von Sicherheitsvorfällen (SO5) 15 Risiken gesteuert werden. Dies kann darauf zurückgeführt werden, dass durch eine frühzeitige Meldung und die Definition entsprechender Prozesse auch frühzeitig Steuerungsmaßnahmen ergriffen werden können, durch die beispielsweise Schwachstellen in Bezug auf Zutrittsrechte, Fehlfunktionen etc. zeitnah geschlossen werden können und somit das Schadensausmaß begrenzt werden könnte.

Steuerungsmaßnahme		**steuerbare Wissensrisiken**	**Σ**
SO1	Richtlinien zur Nutzung von IT-Systemen	VP4, VO7, VE4, DP1, DO2, DE8, DE9	7
SO2	Richtlinien zum Verlassen des Arbeitsplatzes	VP4, VO6, VO7, VE3, DP1, DO1, DO2, DO3, DE7	9
SO3	Richtlinien zur Löschung und Vernichtung von Datenträgern und Dokumenten	VP4, VO6, DP1, DO1	4
SO4	Richtlinien zum Verhalten bei mobiler Arbeit	VP4, VO6, VO7, VE3, VE4, DP1, DO1, DO2, DE7, DE8, DE9	11
SO5	Richtlinien zur Meldung von Sicherheitsvorfällen	VO6, VO7, VS1, VE1, VE3, VE4, DO1, DO2, DS3, DE1, DE2, DE3, DE7, DE8, DE9	15
SO6	Wissenstransferrichtlinien	DP1, TP1	2
SO7	Richtlinien zu Auskünften und Publikationen	DP1, DO5, DE1, DE6	4
SO8	Führung	VP3, VP4, VP5, VE1, DP1, DP2, TP2, TP3	8
SO9	Auswahl der Mitarbeiter	VP4, VP5, DP1, DP2, DE3, TP4, QP3, QO2	8

[248] Für Details zur Behandlung von Software im Urheberrecht siehe (Ensthaler 2003, 7ff).

SO10	Mitarbeiterbindung	VP3, VE1, DE11	3
SO11	Maßnahmen beim Ausscheiden der Mitarbeiter	VO6, VO7, DO1, DO2, DE11	5
SO12	Personalentwicklung	VP4, DP1, TP4, TP5, QP1, QO2	6
SO13	Redundanzschaffung	VP1, VP2, VP3, VO1, VE1, VE2, TO3, QP1, QO3	9
SO14	Einsatz von Genehmigungsprozessen	DP1, DP2, DO5, DE2, DE4	5
SO15	Vier-Augen-Prinzip	VP5, DP1, DP2, QP3	4
SO16	Aufteilung von Wissen	DE6, DE11	2
SO17	Dokumentation	VO2, VO3, VO4, VO5, TO1, TO2	6
SO18	Nachfolgerregeln	VO3	1
SO19	Vertreterregeln	VO4, VE2	2
SO20	Erhaltung informeller Netzwerke	VP1, VP2, VP3, VO8, TO1, TO2, QO1	7
SO21	risikobewusste Auswahl des Kooperationspartners	DE4, TO6, TE1, TE2	4
SO22	risikobewusste Auswahl von Outsourcing-Dienstleistern	DE5, DE10, QE1, QE2	4
SO23	Partnerbindung	DE4	1
SO24	Kontrolle des Partners	DO4, DE4, DE5, DE10, TE2	5
SO25	Begrenzung der personellen Interaktionspunkte	DO5	1
SO26	Validierung dokumentierten Wissens	QP1, QP2, QO5, QO6, QS1, QE1	6
SO27	Verortung dokumentierten Wissens	QP4, QO3, QO6	3
SO28	vertrauensbildende Maßnahmen	TP1, TP2, TP3, TO4, TO5, TS3, TE2, TE3	8
ST1	Sicherung der IT-Systeme	VE4, DS1, DE9, TS3, QS4, QE3	6
ST2	Wartung der IT-Systeme	VS1, DS3, TS2, QS1, QS2, QS3	6
ST3	Datensicherungskonzept	VP4, VP5, VS2, VE3, VE4, VE5	6
ST4	Einsatz von Verschlüsselungsverfahren	DS1, DE7, DE8, DE9	4
ST5	Zugriffskontrollen	VO7, DO2, QE3	3
ST6	Zutrittskontrollen	VO6, DO1	2
ST7	Maßnahmen zur Abwehr von Reverse Engineering	DE6	1
ST8	Maßnahmen zum Abhörschutz	DE8	1
ST9	Einsatz technischer Nutzungsbeschränkungen	VP5, VE3, DE11	3
ST10	Digitales Rechtemanagement	DO2, DO4, TO4	3
ST11	Sicherstellung hoher Medienqualität	TS1, TS2, QS1, QS2, QE2	5
SR1	Geheimhaltungsvereinbarungen	DP1, DP2, DE1, DE3, DE5, DE11	6
SR2	Konkurrenzschutzklauseln	VP3, DE3, DE11	3
SR3	Kooperationsvereinbarungen	DE4, DE5, TE2, TE3	4
SR4	vertragliche Regelungen für externe Dienstleister	DE5, QE1, QE2	3
SR5	Abwehr von Betriebsspionage /-sabotage	DE2, DE3, DE4, DE7, DE8, DE9	6
SR6	gewerbliche Schutzrechte	DE6	1

Tab. 14 Steuerungsmaßnahmen und steuerbare Wissensrisiken

Mobile Tätigkeiten bergen erhöhte Risiken in sich, da beispielsweise Endgeräte gestohlen bzw. liegen gelassen werden oder der Zugriff auf IT-Systeme über ungesicherte Verbindungen erfolgt. Aus diesem Grund könnten Richtlinien zum Verhalten bei mobiler Arbeit (SO4) einen positiven Beitrag zur Risikobegrenzung leisten. Nach plausiblen Überlegungen dürften 11 Wissensrisiken mit einer derartigen Maßnahme steuerbar sein. Weiterhin könnten Richtlinien zum Verlassen des Arbeitsplatzes (SO2) in Bezug auf neun Wissensrisiken einen positiven Beitrag zur Reduktion der entsprechenden Risikoerwartungswerte leisten, da so beispielsweise durch Abschließen der Büros bzw. Passwortsicherung der PCs Wissensrisiken entgegengewirkt werden kann, die sich aus Zutritts- und Zugriffsverletzungen ergeben. Darüber hinaus könnten durch die Maßnahme Redundanzschaffung v.a. die Wissensrisiken, die im Zusammenhang mit verschiedenen Ausprägungen der Fluktuation (z.B. Nachfolgeverlust, Un-

ternehmenswechsel) stehen, reduziert werden. Dieser positive Beitrag trifft nach plausiblen Überlegungen auf neun Wissensrisiken zu. Die weiteren Einflüsse können Tab. 14 entnommen werden. Betrachtet man die Zusammenhänge invers, so bestehen Wissensrisiken, zu deren Reduktion vergleichsweise viele oder auch eher wenige Maßnahmen herangezogen werden können. Demnach könnten zur Reduktion von Fehlverhalten im Bereich der Wissensdiffusion (DP1) 12 verschiedene Maßnahmen, die z.B. Richtlinien, Führung oder Kontrollen betreffen, eingesetzt werden. Analoges gilt für fahrlässiges Fehlverhalten im Kontext von Wissensverlusten, das möglicherweise durch acht Steuerungsmaßnahmen begrenzt werden kann. Darüber hinaus könnten Wissensrisiken aus Zutritts- (DO1, VO6) und Zugriffsverletzung (DO2, VO7) durch das Ergreifen entsprechender Kontrollen und flankierende Richtlinien reduziert werden.

Wissensrisiken		**einsetzbare Steuerungsmaßnahmen**	**Σ**
VP1	unbegleiteter Ruhestand	SO13, SO20	2
VP2	Beendigung der Erwerbstätigkeit	SO13, SO20	2
VP3	Unternehmenswechsel	SO8, SO10, SO13, SO20, SR2	5
VP4	fahrlässiges Fehlverhalten	SO1, SO2, SO3, SO4, SO8, SO9, SO12, ST3	8
VP5	vorsätzliches Fehlverhalten	SO8, SO9, SO15, ST3, ST9	5
VO1	Reorganisationsverlust	SO13	1
VO2	Nichtdokumentation	SO17	1
VO3	Nachfolgeverlust	SO17, SO18	2
VO4	Vertretungsverlust	SO17, SO19	2
VO5	Übergabeverlust	SO17	1
VO6	Zutrittsverletzung	SO2, SO3, SO4, SO5, SO11, ST6	6
VO7	Zugriffsverletzung	SO1, SO2, SO4, SO5, SO11, ST5	6
VO8	unbegleitete Beendigung der Zusammenarbeit	SO20	1
VS1	technisches Versagen / Fehlfunktionen	SO5, ST2	2
VS2	mangelnde Wiederherstellbarkeit	ST3	1
VE1	Abwerbung	SO5, SO8, SO10, SO13	4
VE2	Personalausfall	SO13, SO19	2
VE3	Diebstahl	SO2, SO4, SO5, ST3, ST9	5
VE4	Angriff auf IT-Systeme	SO1, SO4, SO5, ST1, ST3	5
VE5	höhere Gewalt	ST3	1
DP1	fahrlässiges Fehlverhalten	SO1, SO2, SO3, SO4, SO6, SO7, SO8, SO9, SO12, SO14, SO15, SR1	12
DP2	vorsätzliches Fehlverhalten	SO8, SO9, SO14, SO15, SR1	5
DO1	Zutrittsverletzung	SO2, SO3, SO4, SO5, SO11, ST6	6
DO2	Zugriffsverletzung	SO1, SO2, SO4, SO5, SO11, ST5, ST10	7
DO3	unkontrollierter Einsatz temporärer beschäftigter Mitarbeiter	SO2	1
DO4	unkontrollierte interorganisatorische Zusammenarbeit	SO24, ST10	2
DO5	unkontrollierte Veröffentlichung	SO7, SO14, SO25	3
DS1	mangelnde Sicherung der IT-Systeme	ST1, ST4	2
DS2	technisches Versagen / Fehlfunktionen	SO5, ST2	2
DE1	Aushorchung	SO5, SO7, SR1	3
DE2	Einschleusung	SO5, SO14, SR5	3
DE3	Anwerbung	SO5, SO9, SR1, SR3, SR4	5
DE4	opportunistisches Verhalten der Partner	SO14, SO21, SO23, SO24, SR3, SR5	6
DE5	unzureichende Vertraulichkeitswahrung durch Partner	SO22, SO24, SR1, SR2, SR5	5
DE6	Reverse Engineering	SO7, SO16, ST7, SR6	4
DE7	Diebstahl	SO2, SO4, SO5, ST4, SR5	5
DE8	Abhören	SO1, SO4, SO5, ST4, ST8, SR5	6
DE9	Angriff auf IT-Systeme	SO1, SO4, SO5, ST1, ST4, SR5	6

DE10	Sicherheitsverstoß durch Partner	SO22, SO24	2
DE11	Anwendung von Wissen durch ehemalige Mitarbeiter	SO10, SO11, SO16, ST9, SR1, SR2	6
TP1	Zurückhaltung aufgrund Unsicherheit	SO6, SO28	2
TP2	mangelndes Vertrauen	SO8, SO28	2
TP3	Abwehr- / Vermeidungshaltung	SO8, SO28	2
TP4	unzureichende Explizierung	SO9, SO12	2
TP5	unzureichende Absorbierung	SO12	1
TO1	unbegleitete Reorganisation	SO17, SO20	2
TO2	unbegleitete Beendigung von Projekten	SO17, SO20	2
TO3	fehlende Transparenz über vorhandenes Wissen	SO13	1
TO4	eingeschränkte Zusammenarbeit	SO28, ST10	2
TO5	hemmende Sicherheitsrichtlinien	SO28	1
TO6	Inkompatibilitäten zwischen den Partnern	SO21	1
TS1	Bereitstellung unzureichender Medien	ST11	1
TS2	unzureichende Anwenderfreundlichkeit	ST2, ST11	2
TS3	unzureichende Vertrauenswürdigkeit	SO28, ST1	2
TE1	mangelnde Leistungsfähigkeit des Partners	SO21	1
TE2	mangelnde Leistungsbereitschaft des Partners	SO21, SO24, SO28, SR3	4
TE3	Schutzverhalten des Partners	SO28, SR3	2
QP1	unzureichende Identifikation und Bewertung	SO12, SO13, SO26	3
QP2	unzureichende Erstellung und Weiterverarbeitung	SO26	1
QP3	Manipulation von Inhalten	SO9, SO15	2
QP4	mangelnde Anwendbarkeit von Wissen	SO27	1
QO1	unbegleiteter unternehmensinterner Stellenwechsel	SO20	1
QO2	Mangel an qualifiziertem Personal	SO9, SO12	2
QO3	mangelnde Verfügbarkeit von Kompetenzen	SO13, SO27	2
QO4	unzureichende Gewährleistung der Aktualität	SO26	1
QO5	mangelnde inhaltliche Überprüfung	SO26, SO27	2
QS1	unzureichende Verfügbarkeit von IT-Systemen	SO26, ST2, ST11	3
QS2	zeitaufwändige Bereitstellung	ST2, ST11	2
QS3	unzureichend konsolidierte Quellen	ST2	1
QS4	unzureichende Vertrauenswürdigkeit	ST1	1
QE1	unzureichende Inhaltsqualität der von Dritten bereitgestellten Inhalte	SO22, SO26, SR4	3
QE2	unzureichende Medienqualität der von Dritten bereitgestellten Inhalte	SO22, ST11, SR4	3
QE3	Manipulation der Inhalte durch Dritte	ST1, ST5	2

Tab. 15 Wissensrisiken und einsetzbare Steuerungsmaßnahmen

Ebenso wie bei den Steuerungsmaßnahmen existieren auch Wissensrisiken, die sich vergleichsweise weniger steuern lassen bzw. für die spezialisierte Steuerungsmaßnahmen eingesetzt werden. Diese sind vorwiegend den beiden Konzepten Wissenstransfer und Wissensqualität zuzuordnen. Die Vernetzungen der Wissensrisiken und Steuerungsmaßnahmen in diesem Abschnitt sollen einen ersten Anhaltspunkt liefern, welche Maßnahmen sich potentiell zur Steuerung der Wissensrisiken eignen. Zur Validierung der Zusammenhänge, Eignung und Relevanz der Kategorisierung zu Wissensrisiken und der korrespondierenden Steuerungsmaßnahmen ist ein Einsatz in Unternehmen oder weiterführende empirische Forschung erforderlich. Ausgewählte Sachverhalte werden im Rahmen der empirischen Studie, die Gegenstand der Kapitel 6 und 7 ist, betrachtet. Eine vollständige Evaluierung ist allerdings aufgrund des Umfangs der identifizierten Wissensrisiken, Maßnahmen und der sich daraus ergebenden Maßnahmen im Rahmen dieser Arbeit nicht möglich.

6 Design der empirischen Studie kNOwRISK

In den vorangegangen Abschnitten wurde das Konzept Wissensrisiko erarbeitet und korrespondierende Einzelrisiken sowie Steuerungsmaßnahmen erörtert. Im Rahmen einer empirischen Studie sollen ausgewählte theoretisch gewonnene Erkenntnisse auf ihre Relevanz für Unternehmen überprüft werden, um darauf basierend Handlungsempfehlungen abgeben zu können.

Im Folgenden werden zunächst verwandte empirische Studien (6.1) betrachtet und auf dieser Basis eine Positionierung dieser Studie vorgenommen. Im Anschluss erfolgt die Definition der Primär- und Sekundärziele der Studie und eine Darstellung ihres grundlegenden Aufbaus (6.2). Daraufhin wird das Design der empirischen Studie kNOwRISK[249] vorgestellt und das Vorgehen erläutert (6.3). Abschließend werden bedeutende Aspekte des Abschnittes zusammengefasst und diskutiert (6.4).

6.1 Verwandte empirische Studien

Die detaillierte Betrachtung der Zusammenhänge zwischen der Steuerung von Wissensrisiken und den vier abhängigen Konzepten stellt aufgrund der Neuigkeit einen bisher nicht analysierten Untersuchungsgegenstand dar. Im erweiterten Umfeld bestehen allerdings einige empirische Studien, die bestimmte Teilaspekte des Untersuchungsgegenstandes beleuchten und somit eine gewisse thematische Nähe aufweisen. Dabei können Studien unterschieden werden, die die Steuerung von Wissensrisiken selbst zum Untersuchungsgegenstand haben oder solche, die einzelne Konzepte näher betrachten. Zudem wird in einigen Studien explizit Wissensrisiken als Untersuchungsgegenstand genannt, während andere im erweiterten Umfeld angesiedelt sind. Letztgenannte betreffen beispielsweise die Forschungsgebiete IT-RM oder das Management strategischer Allianzen. Im Folgenden werden Studien, die mit den relevanten Konzepten in Beziehung stehen, erläutert.

Norman (2001) führte eine Studie zum Schutz von Wissen in strategischen Allianzen durch und fokussiert somit direkt auf die Steuerung von Wissensrisiken im interorganisationalen Kontext. Die in der Studie zugrunde gelegten Maßnahmen korrespondieren dabei auch mit den in den Abschnitten 5.10.2-5.10.4 erörterten Maßnahmen und schließen organisatorische, technische und gesetzliche Aspekte ein. Die Studie basiert auf 22 Interviews mit Managern, die in strategische Allianzen involviert sind, und hat eine Priorisierung der Steuerungsmaßnahmen im Hinblick auf deren Effizienz bzw. Eignung zum Schutz von Wissen zum Ergebnis (Norman 2001, 55ff).

Neben der Effektivität von Steuerungsmaßnahmen analysiert Norman in einer weiteren Studie, die auf einem Fragebogen basiert und 61 Allianzen in den Branchen Telekommunikation, Mikroelektronik und Computer als Stichprobe einschließt, Einflussfaktoren auf Risiken in strategischen Allianzen.

[249] Die Durchführung der empirischen Studie wurde durch die Deutsche Forschungsgemeinschaft unter dem Kennzeichen: MA3895/1-1 gefördert.

Beispielhafte Einflussfaktoren sind dabei der Grad der Explizierung des Wissens, die Lernabsicht des Partners, die Zugangsmöglichkeiten für den Partner und die Vertrauensbasis (Norman 2002, 185ff).

Junginger betrachtet im Rahmen einer fragebogenbasierten Studie speziell Risiken im Kontext des Informationsmanagements und analysiert dabei primär die Relevanz verschiedener IT-Risiken und deren Steuerung. Die Studie ist branchenübergreifend auf IT-Manager als Zielgruppe ausgerichtet. Bedingt durch die thematische Nähe des WM zum Informationsmanagement können in Bezug auf IT fokussierte Risiken Anleihen aus dieser Studie genommen bzw. Vergleiche gezogen werden. Diese Studie kann insbesondere Antworten in Bezug auf die Relevanz von Angriffen auf IT-Systeme, Fragen der Verfügbarkeit und andere für den Untersuchungsgegenstand dieser Arbeit relevante Fragestellungen liefern (Junginger 2005, 152ff).

Im Rahmen einer Studie zu Informationsrisiken, die auf Basis eines Fragebogens mit 715 IT-Managern aus Europa und dem mittleren Osten durchgeführt wurde, wurden verschiedene Sachverhalte analysiert, die im Kontext der Konzepte Steuerung und unerwünschte Diffusion stehen. Zentrale Fragestellungen waren neben dem Implementierungsgrad IT-bezogener Steuerungsmaßnahmen der Verlust an Vertraulichkeit oder Ausfall von IT-Systemen (Atherton 2007; Collins, Vile 2007)[250].

Die thematisch am nächsten einzuordnende Studie wurde von Knaese (2004) unter dem Einsatz von Fragebögen durchgeführt. Knaese beschäftigte sich mit Know-how Risiken und untersuchte in der empirischen Studie das Fluktuationsmanagement und im Speziellen Faktoren, die die Fluktuationsneigung von Mitarbeitern und die Mitarbeiterzufriedenheit beeinflussen. Somit steht die Studie im Kontext des fluktuationsbedingten Wissensverlustes und ist auf Großunternehmen im Bankenbereich ausgerichtet, wobei die Stichprobe 591 Mitarbeiter einer Bank mit mehr als 1000 Mitarbeitern umfasst.

In den Jahren 2006 und 2007 wurde am Centre for Research in Innovation Management an der Universität Brighton ein Forschungsprojekt durchgeführt, das das Konzept knowledge leakage als zentralen Untersuchungsgegenstand hat. Knowledge leakage kann nach dem dieser Arbeit zugrunde gelegten Verständnis als ein hybrides Konstrukt aus einer unerwünschten Diffusion und einem Wissensverlust verstanden werden, das neben Risiken aber auch Chancen einschließt (Mohamed et al. 2006, 3). Die Studie ist auf personelle Wissensträger ausgerichtet und nutzt als Erhebungsmethode einen Fragebogen. Eine potentielle Schichtung der Stichprobe und Angaben zur definierten Zielgruppe sind nicht ersichtlich. Auch die Auswertungsergebnisse sind noch nicht verfügbar.

Mansfield untersuchte 1985 speziell das Phänomen der Diffusion von Informationen über neue Technologien. Der Begriff Wissen wird dabei nicht direkt verwendet, jedoch sind das Design der Studie und die entsprechenden Ergebnisse im Kontext der Wissensdiffusion interpretierbar. Mansfield untersuchte primär die Zeit, die verstreicht bis ein Konkurrent Kenntnis von neuen Technologieentwick-

[250] Die Studie wurde durch das Unternehmen Freeform Dynamics (http://www.freeformdynamics.com/) durchgeführt.

lungen nimmt und identifiziert auch potentielle Diffusionskanäle. Die Studie basierte auf Fragebögen und schloss als Zielgruppe 100 Unternehmen des verarbeitenden Gewerbes ein (Mansfield 1985, 217ff).

Zander und Kogut untersuchten in einer Studie Einflussfaktoren auf die Imitierbarkeit von Wissen durch Wettbewerber. Dabei stellen die Kodifizierbarkeit, Komplexität oder Vermittelbarkeit von Wissen beispielhafte Einflussfaktoren dar. Die fragebogenbasierte Studie steht im Kontext der unerwünschten Wissensdiffusion sowie dem dadurch bedingten Verlust an Exklusivität und basiert auf einer Stichprobe von 35 Innovationen[251] (Zander, Kogut 1995, 80ff).

Zum Wissenstransfer bestehen zahlreiche Studien, die herangezogen werden können, da dieses Forschungsfeld seit langem eine hohe Aufmerksamkeit verschiedener Wissenschaftsdisziplinen erfährt. In dieser Arbeit stellt der Erfolg des interorganisatorischen Wissenstransfers, im Sinne einer möglichst umfassenden Replikation des transferierten Wissens beim Empfänger, den zentralen Untersuchungsgegenstand dar. Cummings und Teng untersuchten in einer empirischen Studie Faktoren, die die Charakteristika des Senders, des Empfängers, der Beziehung zwischen beiden und den Transferprozess selbst betreffen und Einfluss auf den Erfolg des Wissenstransfers nehmen. Beispielhafte Faktoren sind die Artikulierbarkeit des Wissens oder die Distanz zwischen den Partnern in Bezug auf die Wissensbasen. Die Studie war auf High Tech Unternehmen in den USA mit mehr als 100 Mitarbeitern ausgerichtet, basierte auf Fragebögen und umfasste eine Stichprobe von 65 Unternehmen, wobei als Ansprechpartner Mitarbeiter in Forschung und Entwicklung definiert wurden (Cummings, Teng 2003, 50ff).

Auch Simonin untersuchte den Wissenstransfererfolg im interorganisationalen Kontext und analysierte den Einfluss von Faktoren wie Schutzverhalten des Partners sowie Spezifität oder Komplexität des Wissens. Im Kontext dieser Arbeit sind insbesondere die Operationalisierung des Wissenstransfererfolges und der Einfluss des Schutzverhaltens des Partners von Relevanz. Die auf Angaben von 147 Unternehmen basierende Studie war an Führungskräfte gerichtet, setzt einen Fragebogen zur Erhebung ein und fokussiert branchenübergreifend auf Unternehmen mit mehr als 500 Mitarbeitern, um sicherzustellen, dass Allianzen für das Unternehmen von Relevanz sind (Simonin 1999, 604ff).

Wathne et al. untersuchen den interorganisatorischen Wissenstransfer und fokussieren dabei die Konstrukte Effektivität des Wissenstransfers und Offenheit. Die empirischen Ergebnisse basieren auf den Aussagen von 62 Kooperationsverantwortlichen aus 45 nordeuropäischen Unternehmen. Im Rahmen dieser Arbeit sind insbesondere die Variablen zur Operationalisierung des Wissenstransfererfolges, die mit den Variablen nach Simonin in etwa gleichlaufen, relevant (Wathne et al. 1996, 66f).

[251] Als Grundgesamtheit wurden 44 Innovationen, die von 20 Unternehmen kreiert wurden, definiert (Zander, Kogut 1995, 80).

Als Vorläufer für Studien und Klassifikationen zur Informations- und Wissensqualität haben Wang und Strong auf der Basis einer mehrstufigen empirischen Studie eine Klassifikation zu Kriterien zur Bestimmung der Datenqualität entwickelt (Wang, Strong 1996). Die Studie legte als Zielgruppe ehemalige MBA Studenten zugrunde, die branchenübergreifend in verschiedenen Unternehmen tätig waren.

Auf der Studie von Wang und Strong basierend haben Lee et al. ein Instrument zum Assessment der Informationsqualität auf der Basis einer mehrstufigen branchenübergreifenden empirischen Studie entwickelt. Dabei schloss die Pilotstudie 52 Personen in sechs Unternehmen und die Hauptstudie 261 Personen in fünf Unternehmen ein. Auf dieser Basis wurden u.a. die Konzepte Zugänglichkeit, Glaubwürdigkeit, Vollständigkeit und Verständlichkeit operationalisiert und Zusammenhänge im Sinne von Korrelationen identifiziert. Insbesondere die Ergebnisse zu den Korrelationen unter den Variablen können zum Vergleich der in dieser Arbeit erarbeiteten empirischen Studie herangezogen werden (Lee et al. 2002). Die verwandten empirischen Studien werden nochmals in Tab. 16 zusammengefasst. Die Ausführungen haben gezeigt, dass zu den verschiedenen Konzepten jeweils Studien bestehen, die in den vorangegangenen Kapiteln ausführlich erläutert wurden. Diese Studien eignen sich zur Operationalisierung der Konzepte und zum reflektiven Vergleich der Ergebnisse.

Vertreter	**Untersuchungsgegenstand**	**Konzept und beispielhafte Variablen**	**Zielgruppe (Branche, Unternehmensgröße, Ansprechpartner)**	**Stichprobe**	**Erhebungsmethode**
(Norman 2001)	Effizienz von Steuerungsmaßnahmen zum Schutz von Wissen	Steuerung • Geheimhaltungsvereinbarungen • Kooperationsvereinbarungen • gewerbliche Schutzrechte	• Branche: übergreifend • UN-Größe: N.N. • Ansprechpartner: (Kooperationsverantwortliche)	n=22	persönliches Interview
(Norman 2002)	Einflussfaktoren auf Risiken in strategischen Allianzen	Steuerung • unerwünschter Zugang für Partner • Internalisierungsabsicht	• Branche: Telekommunikation, Mikroelektronik und Computer • UN-Größe: übergreifend • Ansprechpartner: CEO`s	n=61	Fragebogen
(Junginger 2005)	Untersuchung der Relevanz von IT-Risiken und deren Steuerung	Steuerung • Sicherheitsbewusstsein • Schutz vor Angriffen	• Branche: übergreifend • UN-Größe: übergreifend • Ansprechpartner: IT-Manager	n=76	Fragebogen
(Atherton 2007; Collins, Vile 2007)	Untersuchung der Relevanz von IT-Risiken und deren Steuerung	Steuerung • Sicherheitsbewusstsein • Datensicherung • unautorisierte Zugriffe	• Branche: übergreifend • UN-Größe: mehr als 500 Mitarbeiter • Ansprechpartner: IT-Manager	n=715	Fragebogen
(Knaese 2004)	Einflussfaktoren auf Fluktuationsneigung	Wissensverlust • Mitarbeiter-	• Branche: Banken • UN-Größe: mehr als 1000 Mitarbeiter	n=591	Fragebogen

	und Mitarbeiterzufriedenheit	zufriedenheit • Vergütung • Arbeitsinhalt	• Ansprechpartner: alle Mitarbeiter		
(Mohamed et al. 2006)	Risiken in Bezug auf den Verlust und die Diffusion von Wissen	Wissensverlust / Wissensdiffusion • Abwerbung • Unternehmenswechsel • Absorbtion durch Partner	• Branche: N.N. • UN-Größe: N.N. • Ansprechpartner: N.N.	n=N.N	Fragebogen
(Mansfield 1985)	Diffusion von Informationen zu Technologieentwicklungen	Wissensdiffusion • Diffusionszeit • Diffusionskanäle	• Branche: verarbeitendes Gewerbe • UN-Größe: N.N. • Ansprechpartner: CEO`s	n=100	Fragebogen
(Zander, Kogut 1995)	Imitation durch Wettbewerber in Abh. der Eigenschaften von Wissen	Wissensdiffusion • Reverse Engineering • Interfluktuation • Imitation	• Branche: innovierende schwedische Unternehmen • UN-Größe: N.N. • Ansprechpartner: Ingenieure	n=35	Fragebogen
(Cummings, Teng 2003)	Einflussfaktoren auf den interorga. Wissenstransfer	Wissenstransfer • Kontexteinbettung • Explizierbarkeit • Transfermedien	• Branche: Hochtechnologie • UN-Größe: mehr als 100 Mitarbeiter • Ansprechpartner: F&E Manager	n=65	Fragebogen
(Simonin 1999)	Einflussfaktoren auf den interorga. Wissenstransfer	Wissenstransfer • Erweiterung der Wissensbasis • Beitrag des Wissens • Reduktion von Abhängigkeiten	• Branche: Hochtechnologie • UN-Größe: mehr als 500 Mitarbeiter • Ansprechpartner: CEO, Kooperationsverantwortliche	n=147	Fragebogen
(Wathne et al. 1996)	Einflussfaktoren auf den interorga. Wissenstransfer	Wissenstransfer • Erweiterung der Wissensbasis • Dauer der Partnerschaft • Vertrauen	• Branche: N.N. • UN-Größe: N.N. • Ansprechpartner: Kooperationsverantwortliche	n=62	Fragebogen
(Wang, Strong 1996)	Kriterien zur Beurteilung der Datenqualität	Wissensqualität • Verfügbarkeit • Genauigkeit • Konsistenz	• Branche: übergreifend • UN-Größe: übergreifend • Ansprechpartner: ehemalige MBA Studenten	n=137 n=385 [252]	Fragebogen
(Lee et al. 2002)	Kriterien zur Beurteilung der Informationsqualität	Wissensqualität • Korrektheit • Sicherheit • Interpretierbarkeit	• Branche: übergreifend • UN-Größe: N.N. • Ansprechpartner: Mitarbeiter	n=52 n=261	Fragebogen

Tab. 16 Übersicht zu den verwandten empirischen Studien

In den Studien werden vorwiegend Unternehmen betrachtet, die mehr als 100 Mitarbeiter beschäftigen, während im Hinblick auf den Einbezug der Branchen eine Konzentration auf einzelne Segmente (z.B. Banken) oder auf technologie- und innovationsfokussierte Unternehmen erfolgt. Die verwandten

[252] Die Studie wurde in eine Vor- (n=137) und Hauptstudie (n=385) unterteilt.

empirischen Studien sind zudem eher quantitativ ausgerichtet und setzen demnach als Erhebungsmethode vorwiegend Fragebögen ein. Im Hinblick auf die Definition von Ansprechpartnern im Vorfeld werden vielfach Führungskräfte oder die Unternehmensleitung genannt. Eine integrierte Betrachtung der Konzepte ist zum aktuellen Zeitpunkt noch nicht erfolgt und wird in den nachfolgenden Abschnitten detailliert erläutert.

6.2 Ziele und Aufbau

Die in der Literatur identifizierten Wissensrisiken und Steuerungsmaßnahmen, die in Kapitel 5 erörtert wurden, stellen die Ausgangsbasis für eine empirische Untersuchung in Bezug auf die Steuerung von Wissensrisiken dar. Den zentralen Untersuchungsgegenstand bildet dabei die Steuerung von Wissensrisiken selbst, wobei das Primärziel der empirischen Studie darin besteht, den Einfluss der Steuerung auf die vier Teilkonzepte Wissensverlust, -diffusion, -transfer und -qualität detailliert zu analysieren[253].

Da Wissensrisikomanagement ein emergentes Forschungsfeld ist, kann derzeit nicht von einer breiten Umsetzung entsprechender Steuerungsaufgaben und deren Institutionalisierung in Unternehmen ausgegangen werden. Daher wird ein exploratives Untersuchungsdesign mit einem mehrstufigen Aufbau gewählt und eine Unterteilung in eine Hauptstudie und zwei vertiefende Studien vorgenommen (siehe Abb. 29).

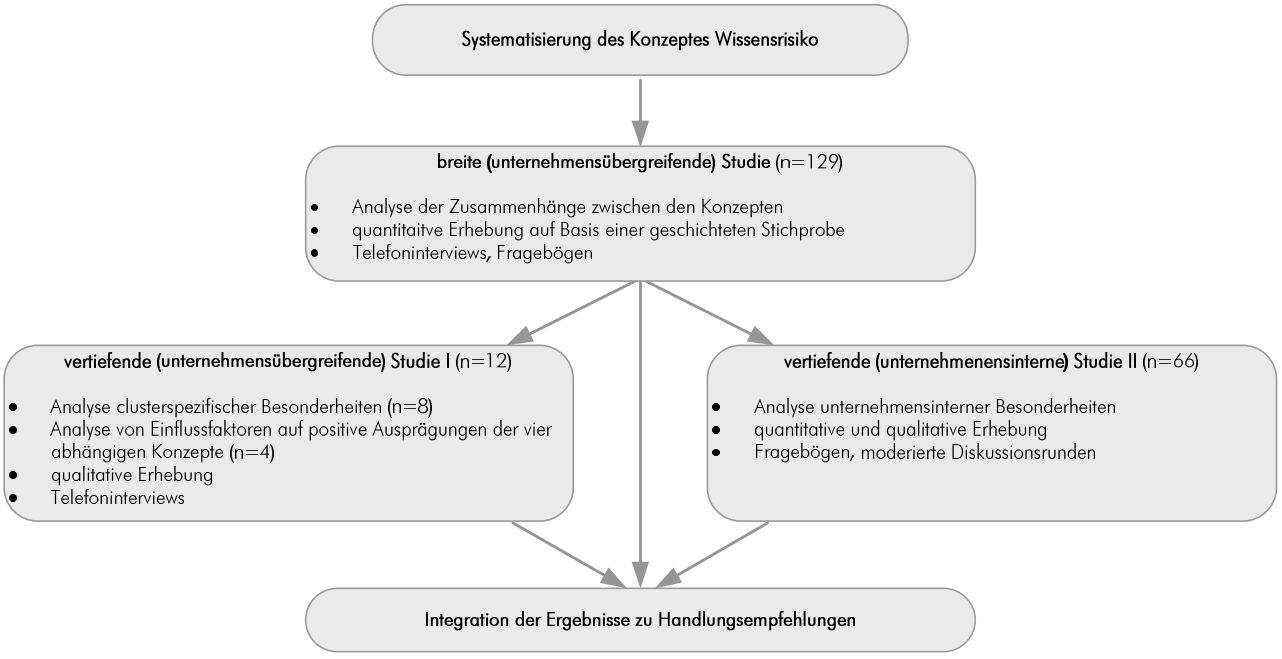


Abb. 29 Aufbau der empirischen Studie

[253] Siehe hierzu auch die Abschnitte 5.3-5.6.

Bezogen auf den Gesamtzusammenhang basiert die Studie auf den theoretischen Erkenntnissen zu Wissensrisiken und Steuerungsmaßnahmen, die in Kapitel 5 erarbeitet wurden und soll im Ergebnis die Ableitung von Handlungsempfehlungen fundieren. Die Hauptstudie basiert auf einer nach Branchen und Größenklassen geschichteten Stichprobe, ist im Hinblick auf den Stichprobenumfang breit ausgerichtet und schließt 129 Unternehmen in Deutschland ein. Ihr Hauptuntersuchungsgegenstand besteht darin, neben deskriptiven Erkenntnissen zur Steuerung, Zusammenhänge zwischen den Konzepten mittels multivariater statistischer Verfahren zu analysieren sowie die Ergebnisse zu interpretieren und daraus konkrete Handlungsempfehlungen zu entwickeln. Dabei sollen diese Zusammenhänge speziell auch durch die Schichtungsmerkmale und den Einfluss weiterer Kriterien, wie z.B. bestehende WM- oder RM-Initiativen, reflektiert werden.

Die Hauptstudie ist quantitativ ausgerichtet, sieht dementsprechend eine Operationalisierung der Konzepte anhand verschiedener Variablen vor und legt als Erhebungsmethode strukturierte Interviewleitfäden zugrunde. Aufgrund der Neuigkeit und des hohen Erklärungsbedarfes des Themengebietes, scheint ein ungerichtetes Versenden des Interviewleitfadens nicht zielführend. Zudem haben schriftliche Befragungen zum Nachteil, dass häufig unklar ist, wer den Fragebogen ausgefüllt hat (Bortz, Döring 2005, 237). Aus diesen Gründen werden als Erhebungsmethodik sowohl Telefoninterviews als auch auf telefonischem Vorkontakt basierende schriftliche Befragung gewählt. Als potentielle Ansprechpartner, für die das Themengebiet Steuerung von Wissensrisiken von Relevanz ist, werden Mitarbeiter definiert, die Stellen in den Unternehmensbereichen Unternehmenssteuerung, -organisation, -kommunikation oder RM besetzen und im Idealfall über eine Berufserfahrung von mehr als drei Jahren im Unternehmen verfügen. Erstgenannte Stellenprofile betreffen im Wesentlichen die Geschäftsführung, während im Bereich der Unternehmensorganisation vielfach auch Fragen des WM verortet sind. Es wird angenommen, dass Mitarbeiter im Bereich der Unternehmensorganisation in der Regel einen guten Überblick über das Gesamtunternehmen und die entsprechenden Prozesse haben und daher ebenfalls geeignete Ansprechpartner sind. Auch Mitarbeiter im Bereich RM dürften mit dem Untersuchungsgegenstand vertraut sein. Zielstellung ist es allerdings, vorwiegend Mitarbeiter der Geschäftsleitung für die Teilnahme an der Studie zu gewinnen.

Telefoninterviews haben im Vergleich zu persönlichen Interviews zum Nachteil, dass sie eine höhere Anonymität aufweisen und keine schriftlichen Unterlagen bzw. bildhafte Vorlagen einsetzbar sind (Gutjahr 1985, 47; Bortz, Döring 2005, 242). Während erstgenannter Nachteil nur schwer kompensierbar ist, soll der zweite Nachteil durch das Versenden des Interviewleitfadens im Vorfeld und die Durchführung des Interviews auf dessen Basis gemindert werden.

Neben das Primärziel treten weitere Sekundärziele. So sollen zum einen deskriptive Erkenntnisse zur Implementierung der Steuerungsmaßnahmen und zur Relevanz der verschiedenen Wissensrisiken gewonnen werden. Weiterhin besteht ein Sekundärziel darin, die Verbreitung von WM- und RM-

Initiativen in Unternehmen zu identifizieren. Zusätzlich zu den in der Literatur thematisierten Steuerungsmaßnahmen sollen auch solche identifiziert werden, die über diese hinausgehen und beispielsweise unternehmensindividuell entwickelt und erfolgreich eingesetzt werden.

Die Hauptstudie wird durch weitere verbundene vertiefende Studien ergänzt, um einerseits Ergebnisse zu reflektieren und andererseits weitere Erkenntnisse zu gewinnen. So wird basierend auf den Daten der Hauptstudie eine Clusteranalyse durchgeführt, um verschiedene Gruppen an Unternehmen zu identifizieren, die Ähnlichkeiten im Hinblick auf die Steuerung von Wissensrisiken und die verschiedenen Konzepte aufweisen. In Abhängigkeit der Ergebnisse werden je Cluster zwei Unternehmen ein zweites Mal kontaktiert, um clusterspezifische Besonderheiten auf der Basis qualitativer Interviews zu erörtern und somit die quantitativen Ergebnisse anzureichern. Darüber hinaus werden unabhängig von der Clusterzuweisung vier Unternehmen, die im Hinblick auf die vier abhängigen Konzepte sehr positive Ausprägungen aufweisen, kontaktiert, um zu identifizieren, auf welche Einflussfaktoren diese Ausprägungen zurückzuführen sind. Somit werden im Falle der unternehmensübergreifenden vertiefenden Studie 12 Unternehmen ein zweites Mal telefonisch befragt.

Primärziel	• Analyse der Zusammenhänge zwischen der Steuerung von Wissensrisiken und den vier Ursachenkategorien von Wissensrisiken sowie Reflexion der Ergebnisse über verschiedene Teilstichproben hinweg	• Hauptstudie
Sekundärziele	• Gewinnung deskriptiver Erkenntnisse zu Steuerungsmaßnahmen und einzelnen Risiken	• Hauptstudie
	• Analyse der Etablierung von WM- und RM-Initiativen	• Hauptstudie
	• Identifikation weiterer Steuerungsmaßnahmen	• Hauptstudie
	• Identifikation clusterspezifischer Besonderheiten in Bezug auf die Zusammenhänge zwischen den Konzepten	• vertiefende Studie I
	• Identifikation von Einflussfaktoren auf positive Ausprägungen zu den vier abhängigen Konzepten	• vertiefende Studie I
	• Identifikation unternehmensinterner Besonderheiten in Bezug auf die Zusammenhänge zwischen den Konzepten	• vertiefende Studie II

Tab. 17 Primär- und Sekundärziele der empirischen Studie

Neben den Besonderheiten, die sich aus der Branchenzugehörigkeit ergeben, sind auch unternehmensinterne Unterschiede in Bezug auf die Einschätzung von Wissensrisiken von Relevanz, die beispielsweise bedingt durch unterschiedliche Perspektiven abweichende Risikowahrnehmung zwischen Hierarchieebenen sowie Unternehmensbereichen bzw. Abteilungen zur Folge hat. Zur Analyse dieser Fragestellungen wird der Fragebogen über die verschiedenen Geschäftsbereiche und Mitarbeitergruppen eingesetzt, wobei der Stichprobenumfang 66 Mitarbeiter einschließt. Um auch gezielt qualitative Erkenntnisse zu gewinnen, erfolgt die Beantwortung des Fragebogens in moderierten Gruppen, in denen entsprechende Anmerkungen seitens der Interviewpartner ermöglicht werden.

Vor dem Hintergrund der auf Basis der Literatur gewonnenen theoretischen Erkenntnisse soll eine Integration der Erkenntnisse der breiten und der vertiefenden Studien in quantitativer und qualitativer

Hinsicht vorgenommen und in Handlungsempfehlungen überführt werden. Die Ziele der empirischen Studie sind in Tab. 17 zusammengefasst und den jeweiligen Studien zugeordnet.
Im nachfolgenden Abschnitt werden auf der Basis des vorgestellten Aufbaus und der Ziele das Design der Studie und das Vorgehen erörtert.

6.3 Design und Vorgehen

Im diesem Abschnitt wird die breite Studie näher erläutert. Dazu werden zunächst die forschungsleitenden Hypothesen erörtert, mittels derer die Zusammenhänge zwischen den in den vorangegangenen Abschnitten erläuterten Konzepten dargestellt werden (6.3.1). Danach werden die Konzepte zur Messung mittels entsprechender Variablen operationalisiert und die dabei zugrunde gelegten Kriterien erläutert (6.3.2). Im Anschluss daran werden Aspekte der Schichtung und Ziehung der Stichprobe erläutert (6.3.3) und das Vorgehen zur Datenerhebung genauer spezifiziert (6.3.4). Der Abschnitt schließt mit der Erörterung von Maßnahmen, die zur Verbesserung der Güte ergriffen wurden (6.3.5).

6.3.1 Hypothesen

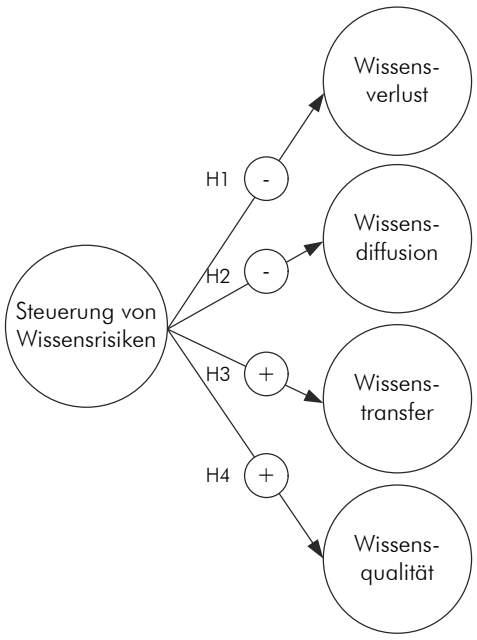


Abb. 30 forschungsleitende Hypothesen

Auf der Basis des in Abschnitt 5.1 entwickelten Konzeptes und dessen Detaillierung in Wissensrisiken und Steuerungsmaßnahmen können vier Hypothesen in Bezug auf die Zusammenhänge zwischen diesen Konzepten formuliert werden. Den Hauptuntersuchungsgegenstand bildet dabei die Steuerung von Wissensrisiken als unabhängiges Konzept, das jeweils auf die vier abhängigen Konzepte Wissensverlust, Wissensdiffusion, Wissenstransfer und Wissensqualität Einfluss nimmt. Die auf der Literatur und Vorüberlegungen basierenden Zusammenhänge sind in den Abschnitten 5.3-5.6 sowie 5.10 dargestellt und werden im Folgenden genauer betrachtet.

Hypothese 1: *Je stärker Wissensrisiken gesteuert werden, desto geringer ist der Wissensverlust.*

Der Verlust von Wissen kann aus Geschäftsprozesssicht z.B. durch die Abwanderung von Mitarbeitern zu anderen Unternehmen, durch das Ausscheiden aus dem Berufsleben oder durch die Versetzung in andere Unternehmensbereiche auftreten. Erfahrungen können durch Nichtdokumentation verloren gehen und dokumentiertes Wissen aufgrund von internen oder externen Ereignissen vernichtet werden. Von einer Steuerung von Wissensrisiken, z.B. Regelungen der Nachfolge

oder der Dokumentation, kann erwartet werden, dass Verluste reduziert bzw. vermieden werden können (siehe hierzu auch die Abschnitte 5.3 sowie 5.10).

Hypothese 2: *Je stärker Wissensrisiken gesteuert werden, desto geringer ist die Wissensdiffusion.*

Abgrenzend zum Wissensverlust ist bei der Diffusion von Wissen dieses noch vorhanden, allerdings nicht exklusiv beim Unternehmen, sondern auch bei Dritten. Diese Nichtexklusivität wirkt sich aus ressourcenbasierter Sicht negativ auf den Wert des Wissens aus. Eine Diffusion kann z.B. auf die persönliche Weitergabe von sensitiven Inhalten oder auf mangelnde IT-Sicherheit zurückzuführen sein. In diesem Zusammenhang wird angenommen, dass durch klare Regelungen zur Bewahrung und Weitergabe von Wissen die Wissensdiffusion reduziert bzw. vermieden wird (siehe hierzu auch die Abschnitte 5.4 sowie 5.10).

Hypothese 3: *Je stärker Wissensrisiken gesteuert werden, desto höher ist der Erfolg des Wissenstransfers.*

Geht man davon aus, dass sich Unternehmen, in denen Wissensrisiken nicht oder vergleichsweise geringer gesteuert werden, im Zweifel in Bezug auf die Weitergabe von sensitiven Inhalten eher rigide verhalten, führt dies zu einer Hemmung des Wissenstransfers. Diese wirkt sich umso stärker aus, je weniger transparent potentielle Empfänger sind, z.B. durch eine Überschreitung von Team-, Abteilungs- und Unternehmensgrenzen. Es wird angenommen, dass im Rahmen der Steuerung von Wissensrisiken Regelungen getroffen werden, die Klarheit darüber schaffen, welches Wissen weitergegeben werden kann und dies positiv auf den Wissenstransfer wirkt (siehe hierzu auch die Abschnitte 5.5 sowie 5.10).

Hypothese 4: *Je stärker Wissensrisiken gesteuert werden, desto höher ist die Wissensqualität.*

Die Steuerung von Wissensrisiken zielt auf die Nachvollziehbarkeit von Prozessen und Entscheidungen und erhöht so den Dokumentationsgrad als relativen Anteil expliziten, dokumentierten Wissens. Wissensrisiken werden durch eine geringe Qualität der Inhalte, der IT-Systeme, die diese bereitstellen, und der Prozesse zu deren Erstellung und Verwendung hervorgerufen. Die Steuerung von Wissensrisiken zielt auf eine Verringerung dieser Defizite, z.B. durch einen besseren Zugang zu aktuellen, korrekten, wiederverwendbaren Informationen und Wissenselementen (siehe hierzu auch die Abschnitte 5.6 sowie 5.10).

Diese vier Hypothesen werden im nachfolgenden Abschnitt operationalisiert, d.h. mit konkreten Variablen zur Messung unterlegt.

6.3.2 Operationalisierung der Konzepte

Wie in Abschnitt 6.2 dargestellt, folgt die breite Studie einer quantitativen Ausrichtung und setzt als Erhebungsinstrument strukturierte Interviewleitfäden ein, die zugleich die Basis für Telefoninterviews und eine schriftliche Beantwortung darstellen. Das in Abschnitt 6.3.1 erläuterte Hypothesenmodell

fokussiert die Zusammenhänge auf der Ebene von Konzepten. Die Messung dieser Zusammenhänge setzt voraus, dass eine oder mehrere Variablen bestimmt werden, die die relevanten Aspekte des zu messenden Konzeptes beschreiben. Die Auswahl muss allerdings in diesem Kontext verschiedenen Anforderungen genügen, die nachfolgend aufgelistet, diskutiert und auf die konkreten Konzepte angewandt werden (siehe Tab. 18).

A	**Literaturbasierung**: Eine Anforderung hinsichtlich der Auswahl der Variablen betrifft die Verankerung in der Literatur. So wird eine Thematisierung der Variable als Voraussetzung gesehen, wobei im Idealfall bereits bestehende Fragen aus anderen Studien bzw. ganze Konzepte übernommen werden. Die beiden letztgenannten Varianten haben zum Vorteil, dass bereits eine Validierung erfolgt ist und dadurch die Güte der Studie erhöht wird (Bryman, Bell 2003, 170ff)[254].
B	**zeitliche Restriktion**: Neben der Literaturbasierung ist bei der Wahl der Variablen in Summe zu beachten, dass die zu deren Beantwortung erforderliche Zeit angemessen ist, um die Teilnahmebereitschaft der Unternehmen möglichst hoch zu halten. Aus diesem Grund wird eine maximale Zeitdauer von 40 Minuten veranschlagt. Legt man geschlossene Fragen als Fragetechnik zugrunde wird mit einem Maximum von 40 Fragen kalkuliert, das im Folgenden beachtet werden muss, wobei der Schwerpunkt der Studie auf das Konzept Steuerung von Wissensrisiken ausgerichtet ist (Gutjahr 1985, 23; Hippmann 1997, 35f).
C	**angemessene Erklärung**: Als weitere Anforderung sollen mithilfe der ausgewählten Variablen die für den Untersuchungsgegenstand relevanten Aspekte des Konzeptes erklärt werden können. Dabei hat die Verwendung einer einzigen Variable vielfach zur Folge, dass aufgrund des hohen Granularitätsniveaus nur ein Teil des Konzeptes abgebildet und gemessen werden kann (Bryman, Bell 2003, 73). Da die in Abschnitt 6.3.1 zueinander in Beziehung gesetzten Konzepte eine hohe Granularität aufweisen, erscheint die Erfassung durch eine Variable nicht zielführend. Neben einer zu hohen Granularität kann aber auch ein zu niedrig gewähltes Granularitätsniveau die Erklärung des Konstruktes negativ beeinträchtigen, da in diesem Fall nur untergeordnete bzw. sehr spezifische Aspekte gemessen werden und eine Vielzahl an Fragen erforderlich wird. Bezugnehmend auf die zeitliche Restriktion (siehe B) werden zur Operationalisierung der fünf zu messenden Konzepte mindestens fünf Variablen eines geeigneten Granularitätsniveaus herangezogen, um die Konzepte hinreichend umfassend zu messen.
D	**Beobachtbarkeit**: Eine weitere Anforderung besteht darin, dass die ausgewählten Variablen beobachtbar sind, da andernfalls bedingt durch vage Schätzungen oder Auslassen der Fragen Verzerrungen auftreten. So sind beispielsweise Fragen im Hinblick auf das Fehlverhalten der Mitarbeiter oder opportunistisches Verhalten von Kooperationspartnern nicht oder nur eingeschränkt beobachtbar. Dabei hängt die Beobachtbarkeit auch davon ab, wie gut die gewählten Variablen mit den für die Befragung definierten Ansprechpartnern korrespondieren.
E	**Antwortbereitschaft**: Neben der Beobachtbarkeit von Variablen ist es auch erforderlich, dass die jeweiligen Ansprechpartner der Zielgruppe auch bereit sind, die Fragen zu den entsprechenden Variablen zu beantworten. Aus diesem Grund ist die Einbeziehung von Variablen, die eine hohe Sensitivität aufweisen oder das Unternehmen bzw. den Ansprechpartner bloß stellen, zu vermeiden, da die Antwortbereitschaft selbst bei Zusicherung der anonymisierten Behandlung gering sein kann (Bortz, Döring 2005, 249)[255].
F	**Beantwortbarkeit**: Da die Studie Unternehmen verschiedener Branchen und Größenklassen einschließt und je Unternehmen ein Ansprechpartner einbezogen werden soll, ist es erforderlich, dass die Variablen so gewählt werden, dass die korrespondierenden Fragen durch einen Interviewpartner beantwortet werden können. Dies bedeutet, dass der Detaillierungs- bzw. Spezialisierungsgrad der Variablen nicht zu hoch gewählt werden darf und die Variablen auch mit dem zu erwartenden Kenntnisstand der Ansprechpartner der Zielgruppe korrespondieren. Zudem hängt die Beantwortbarkeit einer Frage auch entscheidend von deren Formulierung (z.B. Komplexität) ab (Bortz, Döring 2005, 249).

Tab. 18 Anforderungen an die Herleitung der Variablen

[254] Zur Erläuterung von Maßnahmen zur Verbesserung der Güte siehe auch 6.3.5.

[255] In diesem Kontext sind auch Antwortverfälschungen zu beachten, die z.B. auf einer geringen Bereitschaft zur Selbstenthüllung oder auf Motive zur Selbstdarstellung zurückzuführen sind (Bortz, Döring 2005, 250).

Die dargelegten Anforderungen sind allerdings nicht isoliert voneinander zu betrachten, sondern stehen vielmehr zum Teil in einer gegensätzlichen Beziehung. So wird die Anforderung angemessene Erklärung durch die Beobachtbarkeit, Antwortbereitschaft und Beantwortbarkeit limitiert, da Variablen, die zur Messung besonders gut geeignet wären, vielfach nicht beobachtbar sind, aus Gründen der Sensitivität nicht beantwortet werden können oder aufgrund mangelnder Zielgruppenadäquanz nicht beantwortbar sind.

Diese Anforderungen werden bei der nachfolgenden Operationalisierung der Konzepte beachtet, wobei die drei erstgenannten Anforderungen den Gesamtrahmen darstellen und die Anforderungen D-F auf der Ebene der einzelnen Variablen von Relevanz sind. Der Gesamtrahmen gestaltet sich demnach so, dass sämtliche Variablen aus der Literatur abgeleitet und zur Messung des Konzeptes mindestens fünf Variablen herangezogen werden, wobei der zeitliche Rahmen von maximal 40 Minuten Beantwortungszeit, die Gesamtanzahl der Variablen limitiert.

Neben dem so determinierten Gesamtrahmen werden beim Design des Interviewleitfadens und insbesondere der Überführung der Variablen in korrespondierende Fragen zur Messung weitere allgemeine Grundsätze zugrunde gelegt, die nachfolgend erläutert werden. So stehen beim Design des Interviewleitfadens einerseits offene Fragen oder andererseits geschlossene Fragen zur Auswahl. Offene Fragen, also Fragen die im Hinblick auf die Beantwortung keinerlei Einschränkungen vornehmen, weisen vergleichsweise mehr Freiheitsgrade auf und ermöglichen es dem Interviewpartner individuell zu antworten. Geschlossene Fragen geben unterschiedliche Antwortmöglichkeiten vor und weisen in Bezug auf Objektivität, Vergleichbarkeit, Zuverlässigkeit und die Auswertbarkeit Vorteile auf (Holm 1986, 55f; Bortz, Döring 2005, 254f). Dabei kann bei geschlossenen Fragen neben der Vorgabe fester Antworten, die beispielsweise im Hinblick auf die Zahl der Antworten oder die Möglichkeit zu Mehrfachantworten variieren kann, auch der Grad der Zustimmung bzw. die Einstellung erhoben werden (Holm 1986, 35f). Alternativ kann eine Frage auch als Aussage formuliert werden, dem die befragten Personen analog zu Einstellungen in unterschiedlichem Ausmaß zustimmen können. Diese geschlossene Variante wird auch hier aufgrund der oben genannten Vorteile zugrunde gelegt. Dabei können sich derartige Aussagen auf die Person selbst, das Team, die Abteilung oder das Unternehmen beziehen, wobei in diesem Kontext das Unternehmen Hauptgegenstand der Betrachtung ist[256].

Weiterhin bestehen auch im Hinblick auf das Design des Interviewleitfadens und insbesondere in Bezug auf dessen Zusammenstellung und die Formulierung der Einzelfragen weitere Anforderungen, die es zu beachten gilt. Nachfolgend werden speziell Anforderungen betrachtet, die bei der Übersetzung der Variablen in korrespondierende Fragen zum Tragen kommen, während Anforderungen an den

[256] Im Falle von Großunternehmen bzw. Konzernen bezieht sich die Frage bzw. die Aussage auf den jeweiligen Unternehmensteil. Ein entsprechender Hinweis ist auch Gegenstand des Interviewleitfadens (siehe Anhang A 1).

allgemeinen Rahmen am Ende dieses Abschnittes nach der Vorstellung der Operationalisierung der Einzelkonzepte betrachtet werden.

Maßnahmen in Bezug auf eine angemessene Frageformulierung können zum einen beim Design des Interviewleitfadens selbst und zum anderen auf der Basis eines Pretests ergriffen werden. In Bezug auf das Design des Fragebogens wurde darauf geachtet, dass und-, doppelt verneinte, indirekt, unrealistisch, suggestiv, komplex, zweideutig oder sehr allgemein formulierte Fragen ausgeschlossen wurden. Ferner wurde auf hypothetische Formulierungen, quantifizierende Beschreibungen, Fachausdrücke, Fremdwörter, wertbesetzte Begriffe und sensitive Details verzichtet, um die Verständlichkeit der Fragen zu erhöhen (Gutjahr 1985, 19ff; Hippmann 1997, 35f; Diekmann 1999, 412ff; Bryman, Bell 2003, 164ff; Bortz, Döring 2005, 244f, 255f).

Im Rahmen eines Pretests, der mit sieben Personen, die der definierten Zielgruppe (siehe 6.2) angehören, durchgeführt wurde, wurde im Hinblick auf die Frageformulierung überprüft, ob die Fragen einfach beantwortbar sind. Im Speziellen sollte identifiziert werden, ob bei der Beantwortung der Fragen Probleme in Bezug auf deren Verständlichkeit, Interpretierbarkeit oder Sensitivität bestehen. Zudem wurde analysiert, ob eine Beantwortung durch die definierte Zielgruppe möglich ist oder die Fragen zu stark Aufgaben- oder Kenntnisbereiche anderer Ansprechpartner tangieren.

Insgesamt wurde die Beantwortbarkeit der Fragen sowohl in Bezug auf die Zielgruppenadäquanz als auch hinsichtlich der anderen Kriterien als gut eingeschätzt. An einigen Stellen wurden die Fragen präzisiert und gekürzt, um sie für den Interviewpartner schneller erfassbar zu machen.

Unter Zugrundelegung dieser Anforderungen werden nachfolgend die Variablen für die fünf Konzepte hergeleitet. Die jeweiligen Variablen wurden in entsprechende Aussagen überführt, die mittels einer 7 Punkt Likert Skala kodiert und auf der Basis der Erkenntnisse des Pretests angepasst wurden. Dabei werden die jeweiligen Variablen in je einer Tabelle dargestellt und dabei die Literaturbasis vermerkt, wobei im Hinblick auf die Verankerung in der Literatur eine dreistufige Unterteilung vorgenommen wird. So kann die Variable (1) in der Literatur erwähnt sein, (2) eine entsprechende Frage in anderen Studien eingesetzt und auf den Untersuchungsgegenstand angepasst worden sein oder (3) die Übernahme einer identischen Frage erfolgt sein.

Da das Konzept Steuerung von Wissensrisiken den Schwerpunkt der Arbeit und der Studie darstellt, wird ein Großteil der im Hinblick auf zeitliche Restriktionen erhebbaren Fragestellungen auf dieses Konzept allokiert, um insbesondere auch umfassende deskriptive Erkenntnisse zum aktuellen Stand der Steuerung in Unternehmen zu gewinnen. Folglich umfasst dieses Konzept 13 Variablen, die korrespondierend zur Unterteilung in Abschnitt 5.10.1 organisatorische, technische und rechtliche Steuerungsmaßnahmen messen.

Variable	Aussage
organisatorische Maßnahmen	
Klassifikation des Wissens	Es ist genau festgelegt, welches Wissen als vertraulich gilt. [(1) (Liebeskind 1997, 631; Das, Teng 1999, 56; Desouza, Vanapalli 2005, 78f, 87)]
Wissenstransferrichtlinien	Es bestehen klare Richtlinien, welches Wissen über die Unternehmensgrenzen hinaus weitergegeben werden kann (externer Wissenstransfer). [(1) (Hamel et al. 1989, 138; Loebbecke et al. 1999, 20; Desouza, Vanapalli 2005, 80f)]
Begrenzung der Interaktion	Der externe Wissenstransfer ist streng auf ausgewählte Mitarbeiter begrenzt. [(1) (Hamel et al. 1989, 136; Baughn et al. 1997, 104, 112; Liebeskind 1997, 650)]
Redundanzschaffung	Abhängigkeiten von Schlüsselkompetenzen einzelner Mitarbeiter werden stetig durch die gezielte Verbreitung dieser Kompetenzen auf mehrere Mitarbeiter reduziert. [(1) (Bonora, Revang 1993, 202ff; van den Brink 2001, 42f)]
technische Maßnahmen	
Zutrittsbeschränkung	Der Zugang zu sensitiven Unternehmensbereichen ist physisch stark begrenzt. [(1) (Fleischer 1997, 237; Liebeskind 1997, 633f; Desouza, Vanapalli 2005, 81f)]
Zugriffsbeschränkung	Der Zugriff auf elektronisch dokumentiertes Wissen wird stark begrenzt. [(1) (Liebeskind 1997, 633f; Desouza, Vanapalli 2005, 81f)]
Dynamisierung der Zugriffsrechte	Zugriffsrechte auf elektronisch dokumentiertes Wissen werden in regelmäßigen Zeitabständen oder in Abhängigkeit konkreter Anlässe laufend angepasst. [(1) (Rogulla, Walther 2003a, 21; Deloitte 2005, 31; Desouza, Vanapalli 2005, 81f)]
IT-Sicherheitsrichtlinien	Umfassende IT-Sicherheitsrichtlinien für die Mitarbeiter bestehen. [(2) (Ernst&Young 2004, 10; CSI/FBI 2005, 16; Deloitte 2005, 31; PricewaterhouseCoopers 2006, 7)]
IT-Sicherheitsbewusstsein	Die im Rahmen des IT-Sicherheitsmanagements eingeforderten Maßnahmen werden von den Mitarbeitern gewissenhaft umgesetzt. [(2) (Ernst&Young 2004, 12; PricewaterhouseCoopers 2006, 7)]
rechtliche Maßnahmen	
Geheimhaltungsvereinbarungen	Geheimhaltungsvereinbarungen, die die Weitergabe von Wissen an externe Personen regeln, werden umfassend eingesetzt. [(1) (Liebeskind 1997, 632f; Norman 2001, 52ff; Desouza, Vanapalli 2005, 80f)]
Konkurrenzschutzklauseln	Konkurrenzschutzklauseln, die eine Abwanderung zu Konkurrenten für einen bestimmten Zeitraum verbieten, werden umfassend als Bestandteil von Arbeitsverträgen eingesetzt. [(1) (Liebeskind 1997, 634; Rønde 2001, 392, 406)]
Kooperationsvereinbarungen	Kooperationsverträge, die den externen Wissenstransfer regeln, werden umfassend als Absicherung eingesetzt. [(1) (Lei 1993, 36; Liebeskind 1997, 632; de Laat 1999, 209; Norman 2001, 52ff; Erickson, Rothberg 2005, 11)]
gewerbliche Schutzrechte (IP)	Entwickeltes Wissen wird umfassend durch gewerbliche Schutz- und Urheberrechte (Intellectual Property Rights) geschützt. [(1) (Liebeskind 1997, 627; Norman 2001, 52ff; Rønde 2001, 391)]

Tab. 19 Variablen und entsprechende Fragen zum Konzept Steuerung von Wissensrisiken

Die Variablen, deren Auswahl nachfolgend erörtert wird, sind zusammen mit den entsprechenden Aussagen in Tab. 19 zusammengefasst. Die Verankerung in der Literatur bezieht sich auf Desouza und Vanapalli (2005), Liebeskind (1997) und Norman (2001) als Primärquellen und wird punktuell durch weitere Quellen ergänzt. Konkrete Fragen zu den Variablen sind größtenteils nicht verfügbar. Eine Ausnahme bilden die beiden technischen Fragen zum Ausmaß ergriffener IT-Sicherheitsmaßnahmen und deren Umsetzung durch die Mitarbeiter, die auf Studien zur IT-Sicherheit basieren. Die in Tab. 19 dargestellten Maßnahmen spiegeln insgesamt die in der Literatur am weitesten verbreiteten Maßnahmen wider. Im Hinblick auf die in Tab. 18 dargelegten Anforderungen wurden neben der Literaturbasierung insbesondere auch die Anforderungen Beobachtbarkeit (D), Antwortbereitschaft (E) und Beantwortbarkeit (F) herangezogen. So ist die Granularität von Variablen insbesondere im Bereich des IT-RM hoch, da eine Reihe spezifischer Einzelmaßnahmen (z.B. Firewalls, Verschlüsselung) von Relevanz sind. Aus Gründen der Beantwortbarkeit und dadurch bedingt, dass IT-Sicherheitsmaßnahmen nicht den Fokus bilden, wurde insbesondere in diesem Bereich ein hohes Aggregationsniveau gewählt. Einige der in den Abschnitten 5.10.2-5.10.4 erörterten Steuerungsmaßnahmen sind zudem durch eine geringe bzw. eingeschränkte Beobachtbarkeit gekennzeichnet und wurden aus diesem Grund gezielt ausgeschlossen. Dies betrifft z.B. personalwirtschaftliche Maßnahmen, Maßnahmen zur Aufteilung von Wissen oder spezifische Maßnahmen im Rahmen von Kooperationen.

Unter organisatorische Maßnahmen werden Klassifikation des Wissens, Wissenstransferrichtlinien, Begrenzung der Interaktion sowie Maßnahmen zur Redundanzschaffung subsumiert. Die Klassifikation von Wissen kann dabei wie in Abschnitt 5.9.1 dargestellt als Voraussetzung für eine effiziente Umsetzung einiger Steuerungsmaßnahme gesehen werden. Bei den eingeschlossenen technischen Maßnahmen, die eine starke Überlappung zu den organisatorischen Maßnahmen aufweisen, werden das Ausmaß der implementierte Zutritts- und Zugriffsrechte sowie deren Dynamisierung ebenso wie die ergriffenen IT-Sicherheitsmaßnahmen und die Umsetzung durch die Mitarbeiter eingeschlossen. Variablen zur Messung des Ausmaßes rechtlicher Maßnahmen betreffen Geheimhaltungsvereinbarungen, Konkurrenzschutzklauseln, Kooperationsvereinbarungen und ergriffene gewerbliche Schutzrechte.

Nachdem die Variablen zur Messung des Konzeptes Steuerung von Wissensrisiken dargelegt wurden, werden nachfolgend die vier abhängigen Konzepte analog betrachtet.

Wissensverlust: Im Rahmen des Konzeptes Wissensverlust wird sowohl an Personen gebundenes als auch in Objekten inkorporiertes Wissen betrachtet. Hinsichtlich der Variablen, die das Ausmaß von Wissensverlusten in Unternehmen betrifft, sind neben der angemessenen Erklärung die Anforderungen D-F (siehe Tab. 18) von Bedeutung. Daher erfolgt bezugnehmend auf die in Abschnitt 5.3 diskutierten Wissensrisiken eine Konzentration auf Wissensrisiken, die der Ursachenkategorie Organisation

zugeordnet sind, da Variablen dieser Kategorie eine vergleichsweise höhere Beobachtbarkeit aufweisen, da beispielsweise bestimmte Prozesse implementiert sind und korrespondierende Anweisungen bestehen. Im Hinblick auf Wissensrisiken der Ursachenkategorie Personen haben die Ausführungen in Abschnitt 5.3.1 gezeigt, dass Fehlverhalten der Mitarbeiter von besonderer Bedeutung ist. Da dessen Beobachtbarkeit jedoch gering ist, erfolgt ein Ausschluss. Risiken im Bezug auf Systeme betreffen die Datensicherung und das technische Versagen. Bedingt durch die Definition der Zielgruppe der Interviewpartner scheinen Fragen zu diesen Risiken eher ungeeignet. Risiken der Ursachenkategorie externe Ereignisse, wie z.B. Angriffe auf IT-Systeme, sind ebenso schwer beobachtbar, werden evtl. aus Gründen der Reputation nicht wahrheitsgemäß beantwortet und sind zudem nicht zielgruppenadäquat.
So wird zum einen die Nichtdokumentation von Wissen betrachtet, wobei zwischen Projekt- und Tagesgeschäft differenziert wird, da davon ausgegangen wird, dass sich in diesen beiden Bereichen das Dokumentationsbewusstsein bzw. entsprechende Richtlinien unterscheiden. Zum Zweiten werden Risikoereignisse betrachtet, die in Zusammenhang mit einem Stellenwechsel bzw. der temporären Nichtverfügbarkeit des Stelleninhabers stehen. Weiterhin werden Risiken, die sich aus der Nachbesetzung, der Reorganisation und der temporären Vertretung ergeben, eingeschlossen. Zuletzt wird erhoben, inwiefern dokumentiertes Wissen verloren gegangen ist. Dies kann beispielsweise auf IT-Sicherheitsvorfälle oder Fehlverhalten zurückgeführt werden (siehe Tab. 20).

Variable	Aussage
Nichtdokumentation (Tagesgeschäft)	Im operativen Tagesgeschäft entwickeltes Wissen wird umfassend dokumentiert und verfügbar gemacht. [(1) (Zander, Kogut 1995; Desouza, Vanapalli 2005, 84)]
Nichtdokumentation (Projektgeschäft)	In Projekten entwickeltes Wissen wird umfassend dokumentiert und verfügbar gemacht. [(1) (Disterer 2002, 517; Schindler, Eppler 2003, 221ff)
Nachbesetzung	Bei der Nachbesetzung bestehender Stellen treten erhebliche Einarbeitungsprobleme auf, da das erforderliche Wissen nur schwer bzw. unvollständig rekonstruiert werden kann. [(1) (van den Brink 2001, 66; Knaese 2004, 43), (2) (Romhardt 1998, 374)]
Vertretung	Bei der Vertretung bestehender Stellen treten erhebliche Einarbeitungsprobleme auf, da das erforderliche Wissen nur schwer bzw. unvollständig rekonstruiert werden kann. [(1) (van den Brink 2001, 66)]
Reorganisation	Durch die Reorganisationen von Projektteams, Abteilungen oder Geschäftsbereichen steht Wissen, das benötigt wird, in erheblichem Ausmaß nicht zur Verfügung. [(1) (Knaese 2004, 52)]
Verlust dokumentierten Wissens	Dokumentiertes Wissen ist häufig nicht wiederherstellbar verloren gegangen. [(1) (Desouza, Awazu 2004, 3); (2) (Paulus 2000, 397)]

Tab. 20 Variablen und entsprechende Fragen zum Konzept Wissensverlust

Wissensdiffusion: Wissensdiffusion wird ebenso wie der Wissensverlust durch eine Reihe an Variablen gemessen, die mit den in Abschnitt 5.4 dargestellten Wissensrisiken korrespondieren. Eine angemessene Erklärung des Konzeptes (siehe Anforderung B in Tab. 18) wird in diesem Fall insbesondere durch die eingeschränkte Beobachtbarkeit erschwert, die daraus resultiert, dass vielfach verschiedene

Akteure, wie z.B. Konkurrenten, im Hintergrund handeln und so eine auf Unternehmensebene unbewusste Diffusion verursachen. Aus diesem Grund schließt die Operationalisierung (siehe Tab. 21) zum einen verschiedene Kanäle, über die Wissen diffundiert, und zum anderen beobachtbare Ergebnisse einer erfolgreichen Diffusion als Variablen ein. Letztere können ein Indiz dafür sein, dass Wissen über verschiedene beobachtbare und nicht beobachtbare Ereignisse diffundiert ist. Zur Fundierung der Variablen werden verschiedene Autoren herangezogen, wobei die Arbeiten von Kogut und Zander[257], die sich mit Fragen der Imitation, Produktbeobachtbarkeit und des Reverse Engineering im Kontext von Technologien auseinandersetzen, bei vier der sechs Variablen zur Fundierung herangezogen werden können.

Variable	Aussage
Kanäle der Wissensdiffusion	
unautorisierte Zugriffe	Unautorisierte Zugriffe auf elektronisch dokumentiertes Wissen treten häufig auf. [(1) (Ernst&Young 2004, 10f; Deloitte 2005, 31; Desouza, Vanapalli 2005, 81f)]
nachteilige Mitarbeiterfluktuation	Die Abwanderung qualifizierter Mitarbeiter gereicht stark zum Vorteil für Konkurrenten. [(2) (Zander, Kogut 1995, 89)[258]]
unerwünschter Zugang für Partner	Beim externen Wissenstransfer erlangen Partner in erheblichem Ausmaß Zugang zu Wissen, das ihnen aus Gründen der Vertraulichkeit nicht zugänglich sein sollte. [(1) (Kogut, Zander 1992, 393; Baughn et al. 1997, 105; Norman 2002, 197ff)]
Competitive Intelligence	Konkurrenten gelingt es in erheblichem Ausmaß vertrauliches Wissen über Ihr Unternehmen zu sammeln. [(1) (Liman 1999, 46; Erickson, Rothberg 2005, 13)]
Ergebnisse der Wissensdiffusion	
Reverse Engineering	Das den Produkten / Dienstleistungen zugrunde liegende Wissen wird von Konkurrenten schnell rekonstruiert. [(2) (Zander, Kogut 1995, 88)[259]]
Imitation	Konkurrenten gelingt es erfolgreich Produkte / Dienstleistungen Ihres Unternehmens zu imitieren. [(1) (Zander, Kogut 1995, 76, 78; Teece 2002, 15)]

Tab. 21 Variablen und entsprechende Fragen zum Konzept Wissensdiffusion

Analog zum Wissensverlust werden Risiken, die den Ursachenkategorie Personen und Systeme zugeordnet sind, ausgeklammert, da im erstgenannten Fall Fehlverhalten der Mitarbeiter schwer zu beobachten ist bzw. detaillierte Auskünfte nicht zu erwarten sind. Zudem ist in Bezug auf Aussagen zu technischen Systemen bzw. zur IT-Sicherheit die definierte Zielgruppe nicht adäquat. Die Variablen

[257] Siehe (Kogut, Zander 1992; Zander, Kogut 1995).

[258] Frage im Original: Have any of your skilled manufacturing people left your company to the benefit of competitors after the introduction of the product.

[259] Zander und Kogut teilen die Variable im Original in drei spezifische Teilfragen auf:
a) A competitor can easily learn how to manufacture our product by analyzing descriptions of our product in product catalogues etc.
b) A competitor can easily learn how to manufacture our product by taking it apart and examining it carefully.
c) A competitor can easily learn how to manufacture our product by testing in use.

sind daher wiederum auf die Ursachenkategorie Organisation sowie auf beobachtbare externe Faktoren ausgerichtet.

Wissenstransfer: Das Konzept Wissenstransfer ist, wie in Abschnitt 5.5 dargestellt, im Vergleich zu den anderen Konzepten stärker beforscht und teilt sich allerdings in verschiedene Teildisziplinen auf. So betrachten einige Studien vorwiegend den unternehmensinternen Wissenstransfer, während andere speziell auf interorganisatorischen Wissenstransfer z.B. in Kooperationen oder Joint Venture ausgerichtet sind. Letzterer stellt auch in diesem Kontext den Fokus dar.

Als Variablen zur Messung wird dabei ein vollständiges Set von Simonin herangezogen, wobei die Fragen nur übersetzt und geringfügig an den Untersuchungsgegenstand angepasst sind (siehe Tab. 22)[260]. Dieses Set wird durch zwei weitere Variablen zur Bestimmung der Zufriedenheit aus qualitativer und quantitativer Hinsicht ergänzt. Da dieses Set an Variablen bereits erfolgreich im Rahmen einer empirischen Studie eingesetzt und entsprechend vorvalidiert wurde, werden die Anforderungen, die in Tab. 18 definiert wurden, als erfüllt angesehen.

Variable	Aussage
Beitrag des Wissenstransfers	
Erweiterung der Wissensbasis	Durch externen Wissenstransfer wurde viel Wissen des Partners erlernt. [(3) (Simonin 1999, 621)[261]] ähnlich: [(2) (Wathne et al. 1996, 75)]
Beitrag externen Wissens	Das durch externen Wissenstransfer mit Partnern erworbene Wissen wird angepasst und trägt zu anderen Projekten, Prozessen bzw. Aufgaben stark bei. [(3) (Simonin 1999, 621)[262] ähnlich: [(2) (Wathne et al. 1996, 75)]
Reduktion der Abhängigkeit vom Partner	Im Verlauf der Partnerschaft ist das ursprüngliche Verlassen auf das Wissen bzw. die Abhängigkeit vom Wissen des Partners stark zurückgegangen. [(3) (Simonin 1999, 621)[263]]
Zufriedenheit	
Qualität externen Wissens	Die Qualität des durch externen Wissenstransfer erworbenen Wissens ist gut. [(2) (Cummings, Teng 2003, 62) (1) (Pedersen et al. 2003, 83)]
Quantität externen Wissens	Der Umfang des durch externen Wissenstransfer erworbenen Wissens ist hoch. [(1) (Cummings, Teng 2003, 41f; Pedersen et al. 2003, 83)]

Tab. 22 Variablen und entsprechende Fragen zum Konzept Wissenstransfer

Wissensqualität: Variablen zur Messung des positiv belegten Konzeptes Wissensqualität können unter Zugrundelegung des Modells von Eppler (2003c) vier Ebenen zugeordnet werden (siehe Abb. 25, Seite 180). Das gesamte Modell von Eppler spiegelt das Konzept der Informationsqualität angemessen wider. Dessen erfolgreicher Einsatz im Rahmen verschiedener Fallstudien[264] lässt auch eine

[260] Auch Wathne et al. (1996) messen den Wissenstransfer ähnlich.
[261] Original: Your company has learned a great deal about the technology/process know-how held by your partner.
[262] Original: The technology/process know-how held by your partner has been assimilated by your company and has contributed to other projects developed by your company.
[263] Original: Your company has greatly reduced its initial technological reliance or dependence upon the partner since the beginning of the alliance.
[264] Siehe hierzu auch (Eppler 2003c, 185ff).

Erfüllung der Kriterien Beobachtbarkeit, Antwortbereitschaft und Beantwortbarkeit schließen (siehe Tab. 18). Aus diesem Modell werden die für den Untersuchungsgegenstand relevanten Variablen ausgewählt, wobei sich aus der Anforderung zeitliche Restriktion ein Maximum von sechs Fragen je Wissensrisikoursache ergibt, das die Auswahl limitiert. Variablen dieser Kategorie gehen dabei vollständig auf Eppler zurück, wobei deren Formulierung an die Erfordernisse der Studie und des Untersuchungsgegenstandes angepasst wurde. So wurden die Fragen von Eppler in entsprechende Aussagen umformuliert und die erforderliche Anpassung hinsichtlich der Stärke der Aussagen vorgenommen, um eine Likert Skalierung vornehmen zu können. Die beiden Ebenen[265] Güte und Prozess werden im Vergleich zu den Ebenen Community und Infrastruktur aufgrund ihrer Relevanz für den Untersuchungsgegenstand bevorzugt herangezogen (siehe Tab. 23).

Variable	Aussage
Güte	
Korrektheit	Die Korrektheit des dokumentierten Wissens ist hoch. [(1) (Kahn et al. 2002, 187), (2) (Eppler 2003c, 74)[266]]
Aktualität	Die Aktualität des dokumentierten Wissens ist hoch. [(2) (Eppler 2003c, 74)[267], (1) (Naumann, Rolker 2000, 153; Kahn et al. 2002, 185, 187; Neus 2003, 44)]
Prozess	
Nachvollziehbarkeit	Es ist gut überprüfbar, woher das dokumentierte Wissen stammt bzw. wer verantwortlich ist. [(2) (Eppler 2003c, 74)]
Rechtzeitigkeit	Dokumentiertes Wissen wird ohne Verzögerung zur Nutzung bereitgestellt. [(2) (Eppler 2003c, 74)]
Community	
Anwendbarkeit	Von anderen Mitarbeitern dokumentiertes Wissen kann leicht wieder angewandt werden. [(2) (Eppler 2003c, 74)[268], (1) (Kahn et al. 2002, 187)]
Infrastruktur	
Verfügbarkeit	Auf dokumentiertes Wissen kann bei Bedarf stetig und ungehindert zugegriffen werden. [(2) (Eppler 2003c, 74)[269]]

Tab. 23 Variablen und entsprechende Fragen zum Konzept Wissensqualität

Zusammenfassend werden die fünf Konzepte durch insgesamt 36 Variablen, die als Aussage formuliert und 7 Punkt Likert skaliert sind, operationalisiert (siehe Abb. 31), wobei das Konzept Steuerung von Wissensrisiken mit 13 Variablen den Hauptuntersuchungsgegenstand bildet.

Zusätzlich zu diesen Variablen umfasst der Interviewleitfaden eine ebenfalls Likert skalierte Aussage zur Bedeutung der Ressource Wissen für die Wertschöpfung bzw. die Generierung von Wettbewerbs-

[265] Siehe hierzu auch Abb. 25 in Abschnitt 5.6.1.
[266] Original: Is the information free from distortion, bias and errors?
[267] Original: Is the information up-to-date and not obsolete?
[268] Original (Kombination aus zwei Fragen): Can the information be directly applied? Is the information understandable or comprehensible to the target group?
[269] Original: Is there a continuous and unobstructed way to get the information?

vorteilen, um so die Relevanz von Wissen für das jeweilige Unternehmen zu identifizieren. Darüber hinaus sind drei geschlossene Fragen bezüglich der gesetzlichen Verpflichtung zum RM bzw. zu implementierten RM- und WM-Initiativen Gegenstand des Interviewleitfadens. Zusätzlich sind noch zwei offene Fragen zur Priorisierung der in Abb. 31 dargestellten Steuerungsmaßnahmen sowie zur Ergänzung weiterer Steuerungsmaßnahmen eingeschlossen.

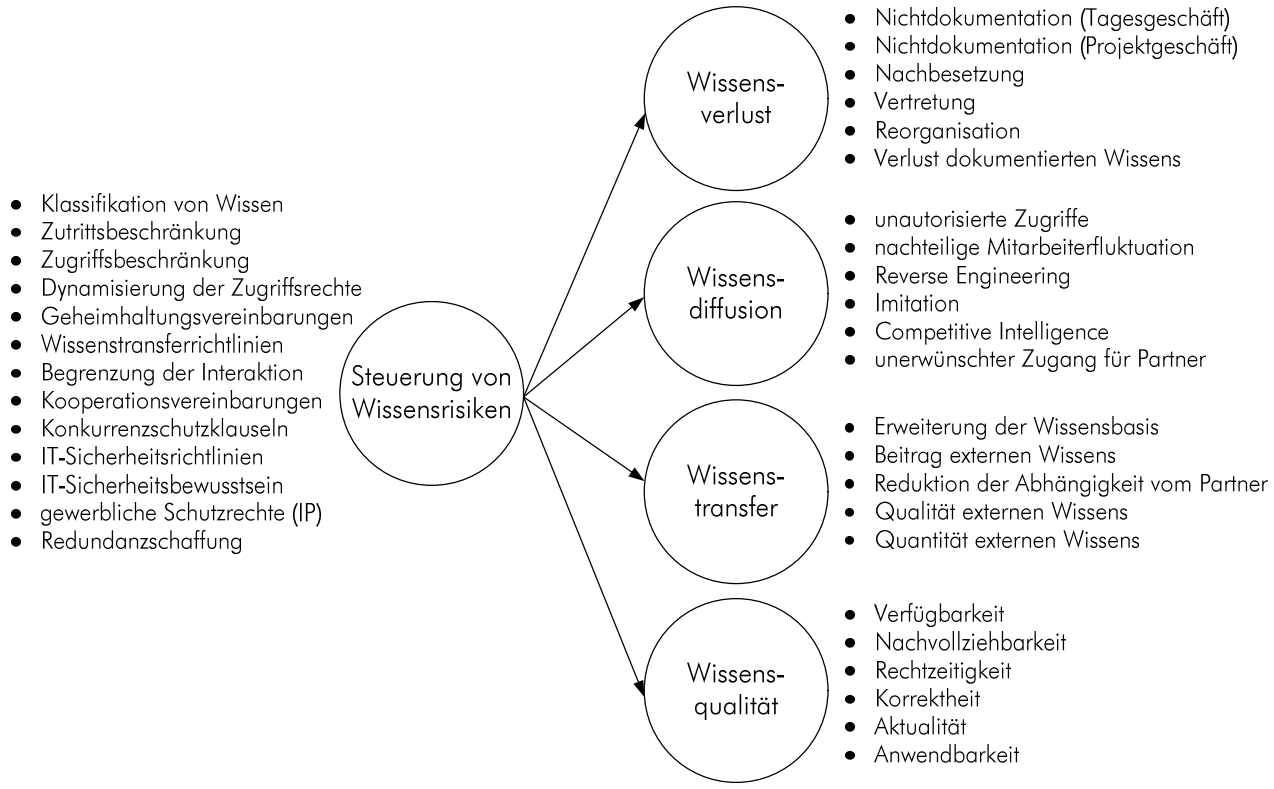


Abb. 31 Operationalisierung der Konzepte

Neben Anforderungen in Bezug auf die konkrete Formulierung der Fragen zu den einzelnen Variablen, wurde auch darauf geachtet, dass der Rahmen des Interviewleitfadens den für empirische Erhebungen definierten Anforderungen genügt. So ist zum einen eine klare Struktur des Interviewleitfadens und eine entsprechende Unterteilung von Fragen zur Person und zum Unternehmen sowie zum eigentlichen Untersuchungsgegenstand erforderlich, wobei letzterer in weitere Blöcke unterteilt werden kann (Hippmann 1997, 35f; Diekmann 1999, 412ff). Eine entsprechende Unterteilung wurde vorgenommen und demnach der Interviewleitfaden neben einer einseitigen Kurzbeschreibung und entsprechenden Kontaktinformationen in die drei Blöcke (1) Angaben zum Unternehmen und zur Person, (2) Wissensrisiken und deren Steuerung sowie (3) WM und RM unterteilt. Block (2) ist dabei inhaltlich weiterhin in die fünf erhobenen Konzepte untergliedert. Da dem Einstieg in ein Interview oder eine schriftliche Befragung bedeutend ist, wurde eine Frage zur Relevanz der Ressource Wissen für

das Unternehmen vorangestellt (Bortz, Döring 2005, 244f). Wie gefordert verläuft dann der Spannungsbogen der erhobenen Variablen so, dass ca. im zweiten Drittel die bedeutendsten Fragen erhoben werden (Diekmann 1999, 412ff). Die Fragetechnik ist in Bezug auf Block (2) einheitlich (Hippmann 1997, 35f).

Entsprechend der Anforderungen verfolgt die vorangestellte Kurzbeschreibung das Ziel, für den Untersuchungsgegenstand und dessen Relevanz für das Unternehmen zu sensibilisieren, Interesse zu wecken und Transparenz hinsichtlich Art und Zweck des Interviews zu schaffen (Gutjahr 1985, 22ff). Darüber hinaus sollen die Teilnehmer über die erforderliche Zeit informiert werden, die im Einklang mit den definierten Anforderungen auf 30-40 Minuten taxiert wurde (Gutjahr 1985, 23; Hippmann 1997, 35f). Die Kurzbeschreibung umfasst zudem den ausdrücklichen Hinweis, dass eine anonymisierte Behandlung der Daten erfolgt (Hippmann 1997, 35f).

Der inhaltliche Aufbau des Fragebogens hat sich in den sieben Pretests bestätigt und wurde von den Interviewpartnern als logisch und in sich stimmig erachtet. Die Kurzbeschreibung wurde auf mehrfache Anregung hin präzisiert. Die vollständige Beantwortung des Interviewleitfadens erforderte zwischen 26 und 37 Minuten und entspricht somit in etwa den Empfehlungen für den Umfang von Fragebögen. Von den Interviewpartnern wurde zudem die Möglichkeit die Fragen während des Interviews mitverfolgen zu können, positiv hervorgehoben. Der vollständige Interviewleitfaden ist dem Anhang (siehe A 1) zu entnehmen.

6.3.3 Schichtung und Ziehung der Stichprobe

Um die Repräsentativität der breiten Studie zu erhöhen, ist die Erfüllung verschiedener Anforderungen im Hinblick auf das Auswahlverfahren der Stichprobe erforderlich. Eine Voraussetzung besteht dabei darin, dass eine klar abgrenzbare Grundgesamtheit besteht. Diese ist im vorliegenden Fall erfüllt, da alle Unternehmen in Deutschland die Grundgesamtheit darstellen. Zum Zweiten ist eine zufällige Ziehung der Elemente der Stichprobe erforderlich, um die Repräsentativität zu erhöhen. Aus diesem Grund werden in dieser Arbeit nur zufällige Auswahlverfahren zur Ziehung der Stichprobe in Erwägung gezogen. Neben der reinen Zufallsauswahl bestehen Mischverfahren wie Schichten-, Klumpen- oder mehrstufige Auswahl (Hippmann 1997, 28ff). Während man bei einer reinen Zufallsstichprobe davon ausgeht, dass jedes Element der Grundgesamtheit a priori über die gleiche Wahrscheinlichkeit verfügt, in die Stichprobe aufgenommen zu werden, wird bei einer geschichteten Stichprobe die Grundgesamtheit nach entsprechenden Merkmalen eingeteilt und innerhalb der Kategorien Zufallsziehungen vorgenommen (Hippmann 1997, 31; Kazmier 1999, 3). Eine Schichtung hat insbesondere bei kleineren Stichprobenumfängen zum Vorteil, dass bei einer stark variierenden Grundgesamtheit die Repräsentativität verbessert wird. Ein weiterer Vorteil besteht darin, dass Unterschiede zwischen den Unternehmen, die auf unterschiedliche Ausprägungen der Schichtungskriterien zurück-

zuführen sind, zusätzlich analysiert werden können. Bezüglich dieser Studie erfolgt eine Schichtung anhand der Kriterien Branchenzugehörigkeit und Unternehmensgröße. Vielfach wird in Studien mit Bezug zum WM eine Einschränkung auf bestimmte Branchen vorgenommen und dies damit begründet, dass die Wissensintensität über Branchen hinweg variiert. Wie in Abschnitt 2.2.6 dargestellt, argumentieren verschiedene Autoren gegen diese Annahme und gehen davon aus, dass die Wissensintensität von branchenunabhängigen Kriterien bestimmt wird (Zack 2003, 67ff).

WZ	Bezeichnung
A	Land- und Forstwirtschaft
B	Fischerei und Fischzucht
C	Bergbau und Gewinnung von Steinen und Erden
D	Verarbeitendes Gewerbe
E	Energie- und Wasserversorgung
F	Baugewerbe
G	Handel
H	Gastgewerbe
I	Verkehr und Nachrichtenübermittlung
J	Kredit- und Versicherungsgewerbe
K	Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen, Erbringung von wirtschaftlichen Dienstleistungen
L	Öffentliche Verwaltung, Verteidigung, Sozialversicherung
M	Erziehung und Unterricht
N	Gesundheits-, Veterinär- und Sozialwesen
O	Erbringung von sonstigen öffentlichen und pers. Dienstleistungen
P	Private Haushalte mit Hauspersonal
Q	Exterritoriale Organisationen und Körperschaften

Tab. 24 Brancheneinteilung nach WZ 2003

Diese Sichtweise wird auch im Kontext dieser Arbeit vertreten und demnach keine Einschränkung nach Branchen vorgenommen, wobei zur Einteilung der Grundgesamtheit in Branchen die für amtliche Statistiken in Deutschland üblicherweise verwendete Klassifikation WZ-2003 herangezogen wird. Diese nimmt auf der obersten Ebene eine Einteilung in 17 Wirtschaftsabschnitte vor und unterteilt diese bis auf fünf Unterziffern über Unterabschnitte oder Wirtschaftsabteilungen hinweg, letztendlich in 1041 Wirtschaftsunterklassen[270]. In diesem Kontext wird zur Klassifikation die oberste Ebene herangezogen, die in die Wirtschaftsabschnitte A bis Q gegliedert ist. In Anlehnung an das Unternehmensregister des Statistischen Bundesamtes werden die Wirtschaftsabschnitte A, B, L, P und Q ausgeklammert. Demzufolge ergeben sich für das erste Klassifikationskriterium 12 unterschiedliche Wirtschaftsabschnitte. Aggregiert man diese nochmals, kann eine Zusammenfassung der Abschnitte C-F und G-O erfolgen, wobei erstgenannte produzierende und die übrigen Wirtschaftsabschnitte dienstleistungsorientierte Branchen repräsentieren.

Als zweites Kriterium zur Schichtung der Stichprobe wird die Größenklasse von Unternehmen herangezogen. Unter Bezugnahme auf die Unternehmenskategorisierung der Europäischen Union (EU 2003) werden Unternehmen in Abhängigkeit der Mitarbeiterzahl in Kleinstunternehmen (1-9 Mitarbeiter), kleine (10-49 Mitarbeiter), mittlere (50-249 Mitarbeiter) und Großunternehmen (≥ 250 Mitarbeiter) unterteilt (siehe Tab. 25)[271]. Basierend auf einer Grundgesamtheit von 3.172.771 Unterneh-

[270] Details zur Klassifikation finden sich unter http://www.statistik-portal.de/Statistik-Portal/klassiWZ03.pdf.

[271] Die EU klassifiziert Unternehmen anhand der Kriterien Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme, wobei zwei der drei Kriterien erfüllt sein müssen. Darüber hinaus müssen die Unternehmen das Unabhängigkeitskriterium erfüllen, um als KMU zu gelten. Unternehmen werden dann als unabhängig eingestuft, wenn sie nicht zu 25% oder mehr

men[272] in Deutschland werden 98,18% der Unternehmen im Hinblick auf das Kriterium sozialversicherungspflichtige Mitarbeiter als Kleinst- oder kleine Unternehmen klassifiziert, wobei erstgenannte mit 90,91% den größten Anteil aufweisen (siehe Tab. 25).

Kriterium / Klasse	Anzahl sozialversicherungspflichtiger Mitarbeiter	Anteil an der Grundgesamtheit (in %)	Anteil an der Stichprobe (absolut)
Großunternehmen	> 249	0,32%	18
Mittlere Unternehmen	≤ 249	1,50%	82
Kleine Unternehmen	≤ 49	7,27%	12
Kleinstunternehmen	≤ 9	90,91%	12

Tab. 25 Klassifizierung von Unternehmen[273]

Wie in Abschnitt 6.1 erörtert, fokussiert ein Großteil der verwandten empirischen Studien auf Unternehmen mit mehr als 100 Mitarbeitern. Dieser grundsätzlichen Ausrichtung auf eine Mindestgröße wird auch in diesem Kontext gefolgt, da insbesondere bei mittleren und großen Unternehmen einerseits eine erhöhte Relevanz von Wissensrisiken und andererseits Ansätze zu deren Steuerung zu erwarten sind. Demnach erfolgt eine Schwerpunktsetzung auf diese beiden Unternehmensgrößenklassen. Legt man eine Zielgröße von 100 Unternehmen als Stichprobe zugrunde, schließt diese bei Errechnung der anteiligen Verteilung 18 Groß- und 82 mittlere Unternehmen ein. Darüber hinaus werden für jeden der 12 Wirtschaftsabschnitte ein Kleinst- und ein kleines Unternehmen eingeschlossen, um potentielle Unterschiede zu den mittleren und großen Unternehmen erkennen zu können. Setzt man beide Schichtungskriterien zueinander in Beziehung ergeben sich insgesamt 48 Kategorien, entlang derer Unternehmen klassifiziert werden können. Tab. 26 ba-

Wirtschaftsabschnitt	Beschäftigtengrößenklassen -9	-49	-249	>250	Σ
WZ-C	2160	602	129	21	2912
WZ-D	215021	47468	14821	3877	281187
WZ-E	8668	802	569	201	10240
WZ-F	278334	30925	2786	183	312228
WZ-G	652034	48158	7682	1229	709103
WZ-H	244199	10666	1231	118	256214
WZ-I	112741	13507	2376	460	129084
WZ-J	41684	1677	1361	766	45488
WZ-K	789147	34767	6842	1205	831961
WZ-M	45605	8956	1731	398	56690
WZ-N	202855	20949	6646	1613	232063
WZ-O	289500	12820	2692	589	305601
Σ	2881948	231297	48866	10660	**3172771**

Tab. 26 Verteilung der Unternehmen in der Grundgesamtheit

des Kapitals oder der Stimmanteile im Besitz von einem oder von mehreren Unternehmen gemeinsam stehen, welche die Definition der KMU bzw. der kleinen Unternehmen nicht erfüllen (Amtsblatt der Europäischen Union 2003, L124/39). Aus Gründen der Verfügbarkeit von Daten seitens des statistischen Bundesamtes wird in dieser Arbeit die Kategorisierung der Unternehmen auf das Kriterium sozialversicherungspflichtige Mitarbeiter reduziert.

[272] Die Grundgesamtheit basiert auf der amtlichen Statistik des statistischen Bundesamtes und bezieht sich zum Stichtag 31.12.2005 auf das Berichtsjahr 2003.

[273] Die Klassifikation basiert auf (EU 2003).

siert auf den Daten des Statistischen Bundesamtes und umfasst zum Stichtag 31.12.2005 Angaben zum Berichtsjahr 2003. Dabei sind alle aktiven Unternehmen mit einem steuerbaren Umsatz und/oder mit sozialversicherungspflichtigen Beschäftigten im Berichtsjahr berücksichtigt.

Legt man diese Verteilung der Grundgesamtheit die in Tab. 25 dargelegte Zielstichprobe zugrunde und betrachtet die insgesamt 59.526 mittleren und großen Unternehmen als Ausgangsgröße, ergibt sich für die entsprechenden 24 Kategorien folgende Verteilung, die im Hinblick auf den Gesamtumfang abweicht (siehe Tab. 27). Bedingt durch den Einbezug der 12 Kleinst- und kleinen Unternehmen wurde ein Minimum von einem Unternehmen je Kategorie definiert. Dies hat zur Folge, dass bei einem Anteilswert von <0,5 in 5 Fällen eine Aufrundung auf 1 erfolgte[274], während bei Anteilswerten über 1 bei der Nachkommastelle < 0,5 eine Abrundung und bei ≥ 0,5 eine Aufrundung erfolgte. Dementsprechend ergibt sich ein Gesamtstichprobenumfang von 129 Unternehmen (siehe Tab. 27).

Wirtschaftsabschnitt	Beschäftigtengrößenklassen -9	-49	-249	>250	Σ
WZ-C	1	1	1	1	4
WZ-D	1	1	25	7	34
WZ-E	1	1	1	1	4
WZ-F	1	1	5	1	8
WZ-G	1	1	13	2	17
WZ-H	1	1	2	1	5
WZ-I	1	1	4	1	7
WZ-J	1	1	2	1	5
WZ-K	1	1	11	2	15
WZ-M	1	1	3	1	6
WZ-N	1	1	11	3	16
WZ-O	1	1	5	1	8
Σ	12	12	83	22	129

Tab. 27 Schichtung der Stichprobe

Die Ziehung der in Tab. 27 dargestellten geschichteten Zufallsstichprobe erfolgte auf der Basis der Unternehmensdatenbank der Creditreform Halle. Dabei wurde in einer ersten Ziehung je Kategorie die zehnfache Anzahl an erforderlichen Unternehmen und somit insgesamt 1290 Unternehmen zufällig gezogen, da von einer Rücklaufquote von 10% ausgegangen wurde. Die Ziehung erfolgte dabei systematisch auf der Basis eines Intervalls, das als Quotient aus der Gesamtanzahl der in der Kategorie verfügbaren Unternehmen der Datenbank und dem erforderlichen Stichprobenumfang ermittelt wurde. Folgt man diesem systematischen Ziehungsmuster, so sind in Bezug auf die mittleren Unternehmen im verarbeitenden Gewerbe (WZ-D / 50-249) 14821 verfügbar und bei einer zehnfachen Überziehung 250 Unternehmensadressen erforderlich.

Dies führt nach dem Ziehungsmuster dazu, dass entsprechend der Berechnung 14.821/250=59,284 jedes 59ste Unternehmen in der Kategorie eingeschlossen wurde. Im Falle einer durch geringere Rücklaufquoten in bestimmten Kategorien der Grundgesamtheit bedingten Nachziehung erfolgte eine analoge Berechnung. Bei Gleichheit der Intervalle wurde das Intervall der Nachziehung um den Wert 1 erhöht.

[274] Eine Aufrundung erfolgte dabei im Falle der Kategorien WZ-C / -249; WZ-C / >250; WZ-E / >250; WZ-F / >250 und WZ-H / >250

6.3.4 Datenerhebung

Basierend auf der zuvor beschriebenen geschichteten Stichprobe wurde eine Adresskartei zusammengestellt, die bezogen auf die Verteilung der Stichprobe (siehe Tab. 27) jeweils die zehnfache Anzahl an Unternehmen einschließt, da eine Rücklaufquote von 10% veranschlagt wurde. Die Adresskartei umfasste in der Ursprungsversion als Kontaktdaten die Postanschrift und die Telefonnummer der gezogenen Unternehmen und wurde im Verlauf der Datenerhebung um eine entsprechende Kontakthistorie ergänzt. Die Datenerhebung erfolgte dabei nach folgendem Muster, das im Kern in die nachfolgend erläuterten Teilschritte unterteilt werden kann.

- **Telefonischer Erstkontakt**: Wie in Abschnitt 6.2 erwähnt, kommt der Sensibilisierung der potentiellen Ansprechpartner für das vergleichsweise junge Forschungsgebiet Wissensrisiko eine besondere Bedeutung zu. Zudem sind die Konzepte so operationalisiert (siehe 6.3.2), dass sie durch Ansprechpartner beantwortet werden sollen, die im Unternehmen bestimmte Stellen bzw. Rollen einnehmen (siehe 6.2). Aus diesen beiden Gründen sieht das Vorgehen zur Datenerhebung einen telefonischen Erstkontakt zu den jeweiligen Unternehmen der Adresskartei vor. Gegenstand dieses Schrittes ist eine kurze Vorabinformation zur Studie in der Telefonzentrale und die Bitte um Vermittlung eines Ansprechpartners, der der definierten Zielgruppe angehört. Dabei wurde auch auf die anonymisierte Behandlung der Daten und in Abgrenzung zu kommerziellen Anbietern die Fokussierung auf Forschungszwecke hervorgehoben (ADM 2005). Als Ergebnis dieses Teilschrittes wurde entweder die Teilnahme an der Studie verweigert oder im Falle einer potentiellen Teilnahme die Kontaktdaten eines Ansprechpartner vermittelt (Durchwahl oder E-Mail Adresse), Informationsmaterial angefordert oder eine interne Weiterleitung des Interviewleitfadens vorgenommen.
- **Kontaktierung des Ansprechpartners**: Falls ein Ansprechpartner vermittelt wurde, erfolgte dessen Kontaktierung per Telefon oder per E-Mail. Im Falle eines telefonischen Kontaktes erfolgte eine Informierung über die Ziele der Studie und deren konkreten Nutzen für das Unternehmen. Als Ergebnis dieses Teilschrittes wurde entweder die Teilnahme an der Studie verweigert oder im Falle einer potentiellen Teilnahme ein Termin für ein Telefoninterview bestimmt oder der Interviewleitfaden an den Ansprechpartner versandt mit der Option, diesen schriftlich zu beantworten.
- **Durchführung des Telefoninterviews / schriftliche Rückantwort**: Je nach Präferenz der Ansprechpartner wurde bei Interesse entweder ein Telefoninterview auf Basis des Interviewleitfadens durchgeführt oder schriftlich an der Studie teilgenommen. Falls ein Telefoninterview durchgeführt wurde, diente der versandte Interviewleitfaden dem Ansprechpartner als Gesprächsgrundlage und Orientierungshilfe.

- **Nachfassanruf bzw. -schreiben:** Bei abgelaufener Deadline und gleichzeitig bekundetem Interesse wurden einige Ansprechpartner erneut per E-Mail oder Telefon kontaktiert. Dabei wurde den Ansprechpartnern eine neue Deadline zur Beantwortung des Interviewleitfadens mitgeteilt.

6.3.5 Maßnahmen zur Verbesserung der Güte

Nachdem der Aufbau der Studie, die Operationalisierung der Konzepte, die Schichtung der Stichprobe und das Vorgehen zur Datenerhebung erläutert wurden, werden in diesem Abschnitt die für die Studie relevanten Gütekriterien sowie entsprechende ergriffene Maßnahmen zu deren Verbesserung erörtert.
Gütekriterien sind nach Lienert (1969, 1ff) von elementarer Bedeutung dafür, ob ein Verfahren als solches im wissenschaftlichen Sinne überhaupt als Test bezeichnet werden kann und geben an, ob die mit ihrer Hilfe gemachten Aussagen wissenschaftliche Aussagefähigkeit besitzen. Im Hinblick auf ihre Wertigkeit kann eine Unterteilung in Haupt- und Nebengütekriterien erfolgen. Zu den Hauptgütekriterien zählen Objektivität, Reliabilität und Validität, während u.a. Normierung, Vergleichbarkeit, Ökonomie und Nützlichkeit des Tests Nebengütekriterien darstellen (Lienert 1969, 10ff; Bortz, Döring 2005, 192).
Die drei Hauptkriterien bauen ausgehend von der Objektivität aufeinander auf, wobei Objektivität besagt, dass ein Test unabhängig vom Untersucher sein muss. Dies bedeutet, dass ein Test zu gleichen Ergebnissen führen muss, wenn er intersubjektiv durchgeführt wird (Lienert 1969, 13f). Reliabilität setzt Objektivität voraus und gibt den Grad der Genauigkeit und Konsistenz an, mit der die Ausprägungen eines Merkmals erfasst werden (Lienert 1969, 14f; Peter 1979, 6; Bryman, Bell 2003, 76). Validität setzt wiederum Reliabilität voraus und betrifft die konzeptionelle Richtigkeit eines Erhebungsinstruments, indem sie angibt, wie gut der Test in der Lage ist, genau das zu messen, was er zu messen vorgibt (Lienert 1969, 16; Churchill 1979, 65; Bortz, Döring 2005, 199).
Einige Maßnahmen zur Verbesserung der Güte werden dabei vorgelagert, also bei der Konzeption und der Durchführung der empirischen Studie ergriffen, während andere Maßnahmen speziell bei der Auswertung zum Tragen kommen. Erstere werden nach einer allgemeinen kurzen Darstellung der für wissenschaftliche Untersuchungen relevanten Gütekriterien in diesem Abschnitt erläutert, während nachgelagerte Maßnahmen Gegenstand von Kapitel 7 sind und an den entsprechenden Stellen thematisiert werden.
Objektivität: Die Objektivität eines Tests gibt an, in welchem Ausmaß die Testergebnisse vom Testanwender unabhängig sind und kann in einer detaillierteren Aufgliederung Objektivität in Durchführungs-, Auswertungs- und Interpretationsobjektivität unterteilt werden (Lienert 1969, 13f). Durchführungsobjektivität ist dann gewährleistet, wenn das Testergebnis von der durchführenden Person unbeeinflusst ist. Die Durchführungsobjektivität kann z.B. durch standardisierte Instruktionen, die dem Testanwender während der Testdurchführung keinen Spielraum lassen, verbessert werden. Auswer-

tungsobjektivität ist dann erfüllt, wenn die Vergabe von Testpunkten durch die auswertende Person unbeeinflusst ist. Verschiedene Auswertende sollen daher bei der Auswertung des Tests auf exakt dieselben Punkte kommen. Die Auswertungsobjektivität hängt von der Art der Itemformulierung ab und wird durch eine klare Vorgabe von Punkten für die entsprechende Antwort erhöht. Interpretationsobjektivität ist gewährleistet, wenn auf Basis der gleichen Auswertungsergebnisse auch die gleichen Schlüsse gezogen werden (Lienert 1969, 13f; Bortz, Döring 2005, 194).

In Bezug auf die empirische Studie kNOwRISK wurde Durchführungsobjektivität dadurch gewährleistet, dass die beteiligten studentischen Hilfskräfte insbesondere im Hinblick auf fachliche Kenntnisse, Kenntnisse zum Aufbau des Fragebogens sowie Gewährleistung der Wertfreiheit geschult wurden, selbst je zwei Pretests durchführten und Rückantworten standardisiert wurden[275]. Auch die Moderatoren, die den Interviewleitfaden im unternehmensinternen Fall einsetzten, wurden entsprechend geschult. Um die Durchführungsobjektivität laufend zu gewährleisten, erfolgte eine regelmäßiger Austausch und die Festlegung eines standardisierten Vorgehens bei entsprechenden Rückfragen (z.B. Angabe identischer Beispiele). Auch die Auswertungsobjektivität wurde im Vorfeld erhöht, da die Variablen zur Messung (siehe Abschnitt 6.3.2) gemäß einer Likert Skala standardisiert wurden. Die Normierung des Tests erhöht auch die Interpretationsobjektivität, da die Freiheitsgrade für die Interviewpartner gering sind.

Reliabilität: Die Reliabilität als Grad der Genauigkeit und Konsistenz eines Instrumentes ist umso höher, je kleiner der zum Messwert gehörende Fehleranteil ist. Ein maximaler Wert ohne Messfehler ist dabei allerdings in der Regel nicht zu erreichen, da Faktoren, wie z.B. situative Störungen oder Müdigkeit, Einfluss nehmen (Bortz, Döring 2005, 195). Reliabilität wird über einen entsprechenden Koeffizienten gemessen, der aussagt, inwieweit die Testergebnisse unter gleichen Rahmenbedingungen reproduzierbar sind (Lienert 1969, 15)[276]. Zur Berechnung der Reliabilität bestehen verschiedene Verfahren.

So gibt die Paralleltest-Reliabilität an, ob ein vergleichbares Messverfahren (z.B. eine vergleichbare Frage) auf der Basis von Korrelationen identische Ergebnisse liefert. Die Bestimmung der Retest-Reliabilität erfolgt durch die Wiederholung der Messung bei Konstanz der zu messenden Eigenschaft und ermittelt die Korrelationen der Ergebnisreihen (Lienert 1969, 15).

Die Innere Konsistenz, die die Homogenität der einzelnen Variablen bezeichnet kann durch die Methode der Testhalbierung und die Konsistenzanalyse bestimmt werden (Lienert 1969, 15). Bei Verwendung der erstgenannten Methode wird der Test in zwei Teile geteilt, den Befragten vorgelegt und die Ergebnisse für jede Testhälfte gesondert ermittelt. Im Anschluss werden die Ergebnisse der beiden Testhälften korreliert und dann auf die Gesamttestlänge hochgerechnet. Die Konsistenzanalyse fasst

[275] In diesem Zusammenhang erfolgte eine Orientierung an den Vorschlägen von (Bortz, Döring 2005, 248)

[276] Abgrenzend zur Validität gibt die Reliabilität nur an, ob der Messwert richtig gemessen wird und nicht ob das Richtige gemessen wird.

die einzelnen Variablen eines Tests als multipel halbierte Testteile auf und behandelt jede Variable wie einen Paralleltest, wobei die Korrelationen zwischen den Variablen dabei die wahre Varianz widerspiegeln (Bortz, Döring 2005, 198). Für die Berechnung wird häufig Cronbachs Alpha eingesetzt, wobei formal der Alpha-Koeffizient der mittleren Testhalbierungs-Reliabilität eines Tests für alle möglichen Testerhebungen entspricht. Alpha ist umso höher, je mehr Items eine Skala enthält und je höher die Itemkorrelationen sind (Bortz, Döring 2005, 198). Reliabilität ist demnach gegeben, wenn ein wesentlicher Anteil der Varianz der einbezogenen Variablen durch die entsprechenden Faktoren erklärt wird (Unterreitmeier, Schwinghammer 2004, 16f).

Konzept	Anzahl Variablen	Cronbachs Alpha
Steuerung	13	0,866
Wissensverlust	6	0,709
Wissensdiffusion	6	0,781
Wissenstransfer	5	0,783
Wissensqualität	6	0,864

Tab. 28 Cronbachs Alpha für die Konzepte

In Bezug auf die empirische Studie kNOwRISK erfolgt eine Ermittlung der Reliabilität auf der Basis Cronbachs Alpha. Der Wert von Cronbachs Alpha kann rechnerisch Werte zwischen minus unendlich und eins annehmen, wobei als Zielwert für eine hinreichende Reliabilität 0,7 definiert wird. In Tab. 28 sind die auf der Basis von SPSS errechneten Alphas je Konzept abgetragen und liegen zwischen 0,709 im Falle des Konzeptes Wissensverlust und 0,866 im Falle der Steuerung. Da der Zielwert nicht unterschritten wird, kann von Reliabilität des Instrumentes ausgegangen werden.

Validität: Das dritte Hauptkriterium Validität dient zur Überprüfung, ob der Test tatsächlich auch misst, was er zu messen vorgibt (Bortz, Döring 2005, 199). Dabei können die drei Hauptarten Inhalts-, Konstrukt- und Kriteriumsvalidität unterschieden werden (Lienert 1969, 255ff). Inhaltsvalidität ist gewährleistet, wenn die gewählten Variablen das zu messende Konstrukt in seinen wichtigsten Aspekten erschöpfend erfassen, wobei die Inhaltsvalidität umso höher ist, je besser die Variablen die Grundgesamtheit der Variablen repräsentieren. Dieses Kriterium, kann nicht berechnet werden, sondern basiert auf subjektiven Einschätzungen, weshalb es auch als Augenscheinvalidität bezeichnet wird (Bryman, Bell 2003, 77; Bortz, Döring 2005, 199). Konstruktvalidität liegt vor, wenn aus dem zu messenden Zielkonstrukt Hypothesen ableitbar sind, die anhand der Testwerte bestätigt werden können (Bryman, Bell 2003, 78; Bortz, Döring 2005, 200). Die Konstruktvalidität kann beispielsweise mittels Faktorenanalyse ermittelt werden. Bei der Überprüfung der Kriteriumsvalidität erfolgt der Vergleich des Testmerkmals mit einem Außenkriterium (Lienert 1969, 17). Kriteriumsvalidität ist somit gegeben, wenn auf der Basis von Ausprägung einer im Test verwendeten Variable auch auf die Ausprägungen einer Variable außerhalb des Tests geschlossen werden kann. Dabei nimmt die Kriteriumsvalidität mit der Korrelation der Variablen zu, wobei ihre Überprüfung nur bei geeignetem Außenkriterium sinnvoll ist (Bortz, Döring 2005, 199f).

In Bezug auf die empirische Studie kNOwRISK wurde die Inhaltsvalidität zum einen durch Beurteilung der eingesetzten Variablen durch Experten gesichert. Zum anderen basieren die Variablen auf der

Literatur und stehen in Zusammenhang mit den jeweiligen Konzepten, weshalb eine Eignung zur Messung der Konzepte unterstellt wird. Dies trifft insbesondere auf das Konzept Wissenstransfer zu, da die zu dessen Messung eingesetzten Variablen bereits in einer empirischen Studie eingesetzt wurden und vorvalidiert sind. Weiterhin kann die Konstruktvalidität auf Basis einer Faktorenanalyse ermittelt werden, die Gegenstand von Abschnitt 7.4.1 ist.

Neben den Hauptgütekriterien stellen die Normierung, Vergleichbarkeit, Ökonomie und Nützlichkeit des Tests Nebengütekriterien dar (Lienert 1969, 19ff). Das Nebengütekriterium Normierung fokussiert auf die Erstellung eines Bezugssystems auf dessen Basis die Ausprägungen der Variablen eines Merkmalsträgers mit einem anderen verglichen und interpretiert werden können. In Bezug auf diese Studie wird ein Vergleich von Ergebnissen einerseits durch die Normierung der Aussagen über eine 7-Punkt Likert Skala und andererseits durch die Ermittlung von Lageparametern der deskriptiven Statistik ermöglicht. Ein Test gilt als ökonomisch, wenn er in der Relation zum Erkenntnisgewinn einen geringen Ressourceneinsatz (z.B. Material, Zeit oder Geld) erfordert, einfach zu handhaben und auszuwerten ist. Im Kontext dieser Studie ist der Ressourcenverbrauch durch den Versand des Interviewleitfadens per E-Mail vergleichsweise gering, während die Handhabung und Auswertung durch die Standardisierung des Interviewleitfadens verbessert wird. Der telefonische Vorkontakt der Ansprechpartner erhöht allerdings den Zeitaufwand der Studie deutlich, schlägt sich allerdings in der Qualität der Antworten wider. Der erforderliche Zeitaufwand aus der Sicht der Befragten ist mit ca. 30-40 Minuten vertretbar und orientiert sich an entsprechenden Empfehlungen aus der Literatur (Gutjahr 1985, 23; Hippmann 1997, 35f). Das Kriterium Nützlichkeit trifft dann zu, wenn Merkmale erhoben werden, für deren Untersuchung ein praktisches Bedürfnis besteht[277]. Die Nützlichkeit der Studie kann einerseits an einer ansteigenden Bedeutung dieses Themenkomplexes in der Literatur und andererseits an den Ergebnissen des Pretests und des Feedbacks der Interviewpartner festgemacht werden.

Im Hinblick auf die drei Hauptgütekriterien wurden im Vorfeld der Studiendurchführung insbesondere Maßnahmen zur Sicherstellung der Objektivität ergriffen. So wurde durch die Standardisierung des Vorgehens und die Schulung der Hilfskräfte die Durchführungsobjektivität verbessert, während Auswertungs- und Interpretationsobjektivität insbesondere durch die Standardisierung des Interviewleitfadens und die dadurch bedingte Reduktion der Freiheitsgrade erreicht wurde. Dem Kriterium Reliabilität wird bei der Auswertung durch die Errechnung von Cronbachs Alpha Rechnung getragen. Die Validität wird durch die im Vorfeld überprüfte Inhaltsqualität sichergestellt.

[277] Weitere Nebengütekriterien sind bei (Schermelleh-Engel 2006) zu finden.

6.4 Zusammenfassung und Diskussion

Im Rahmen dieses Kapitels wurden zunächst verwandte empirische Studien betrachtet. Dabei hat sich gezeigt, dass zum aktuellen Zeitpunkt keine integrierte Betrachtung der in den Kapiteln 5 und 6 dargelegten Zusammenhänge vorliegt, sondern vielmehr auf einzelne Konzepte den Untersuchungsgegenstand bilden, wobei zu jedem der Konzepte empirische Arbeiten bestehen. Die verwandten empirischen Studien fokussieren zumeist auf Großunternehmen, schränken die einbezogenen Branchen ein und setzen Fragebögen zur Erhebung ein. Auch die Studie kNOwRISK ist auf Unternehmen mit mehr als 50 Mitarbeitern ausgerichtet, da ab dieser Mitarbeiterzahl eine höhere Relevanz des Themas und ein höheres Risikopotential vermutet wird. Eine Einschränkung in Bezug auf die einbezogenen Branchen erfolgt im Rahmen dieser Studie allerdings nicht, da davon ausgegangen wird, dass die Bedeutung der Ressource Wissen durch branchenunabhängige Kriterien beeinflusst wird. Um diese beiden Kriterien einzubeziehen, wurde die Stichprobe nach Branchen und Größenklasse geschichtet und eine zufällige Ziehung vorgenommen. Der primär quantitativen Erhebung durch Fragebögen wird auch in diesem Kontext gefolgt, wobei aufgrund der Neuigkeit des Themengebiets ein telefonischer Vorkontakt zur Erklärung der relevanten Fragestellung und zur Identifikation geeigneter Ansprechpartner als besonders bedeutend erachtet wird. Dabei ist insbesondere die Sicherstellung einer hohen Antwortqualität von Relevanz. Um auch qualitative Aspekte zu berücksichtigen, kann sowohl ein Telefoninterview als auch eine schriftliche Beantwortung des Interviewleitfadens erfolgen, wobei erstgenannte Variante präferiert wird, um den Untersuchungsgegenstand durch qualitative Aspekte anzureichern. Die quantitative Erhebung wird zudem durch zwei vertiefende Studien ergänzt, die zum einen unternehmensinterne Besonderheiten der Zusammenhänge betrachten und zum anderen basierend auf einer Clusteranalyse auf Besonderheiten von Gruppen fokussieren. Um die Qualität der Ergebnisse zu erhöhen, wurden im Vorfeld Maßnahmen zur Verbesserung der Güte durchgeführt, wobei diese insbesondere das Kriterium Objektivität betreffen.

7 Auswertung der empirischen Studie kNOwRISK

Die Auswertung der im Rahmen der empirischen Studie gewonnenen Daten schließt verschiedene Aspekte ein und gliedert sich im Wesentlichen in fünf unterschiedliche Auswertungsschwerpunkte (siehe Abb. 32). Dabei betreffen die Auswertungen zum einen die gesamte Stichprobe der 129 Unternehmen und zum anderen eine Auswahl aus diesen, die auf Ergebnisse vorhergehender Analysen zurückgeführt werden kann. So erfolgt einerseits eine deskriptive Analyse der einzelnen Variablen, die zur Messung der fünf Konzepte dienen (siehe Abschnitt 7.2). Dabei werden zur genaueren Analyse unterschiedliche Lage- und Streuungsparameter herangezogen und insbesondere die Variablen genauer betrachtet, die vergleichsweise hohe bzw. niedrige Werte annehmen. Zudem werden diese Ergebnisse hinsichtlich der durch die Schichtung nach Unternehmensgröße und Branchenzugehörigkeit bedingten Einteilung in verschiedene Kategorien erörtert und dabei der Einfluss dieser Kriterien analysiert. Analog dazu wird der Einfluss von Initiativen zu WM und RM analysiert. In diesen Fällen wird mittels induktiver Statistik die Signifikanz von Abweichungen verschiedener Teilstichproben überprüft. Zusätzlich werden die Ergebnisse um qualitative Anmerkungen der Interviewpartner aus den Telefoninterviews oder den offenen Fragen der Fragebögen ergänzt.

Im Anschluss daran werden ausgewählte Einflüsse der Steuerungsmaßnahmen untersucht, um einerseits zu identifizieren, inwieweit die Implementierung von Maßnahmen negative Effekte aufweist. Andererseits soll auf empirischer Basis identifiziert werden, wie gut die Wissensrisiken durch die in der Studie eingeschlossenen Maßnahmen gesteuert werden können (siehe Abschnitt 7.3).

Als weiterer Auswertungsschwerpunkt werden für alle 129 Unternehmen der Stichprobe auf der Ebene der Konzepte Zusammenhänge zwischen diesen unter Einsatz multivariater Verfahren analysiert (siehe Abschnitt 7.4). Dabei wird zum einen eine Faktorenanalyse durchgeführt, um Zusammenhänge zwischen den zur Operationalisierung der Konzepte herangezogenen Variablen zu entdecken. Darüber hinaus sollen im Rahmen einer Clusteranalyse Gruppen an Unternehmen identifiziert werden, die Ähnlichkeiten in Bezug auf die Ausprägungen der Variablen bzw. Konzepte aufweisen.

Diese beiden Auswertungen über alle 129 Unternehmen hinweg werden durch vertiefende Studien ergänzt, wobei die Auswahl der detailliert betrachteten Unternehmen auf den vorangegangen Analysen basiert und sowohl unternehmensinterne als auch unternehmensübergreifende Aspekte einschließt (siehe Abb. 32). Im Hinblick auf die unternehmensübergreifende Vertiefung der Studie werden auf der Basis der Ergebnisse der Clusteranalyse die Besonderheiten der jeweiligen Cluster mit je zwei Unternehmen, die dem Cluster zugeordnet sind und dessen Ausprägungen möglichst gut repräsentiert, mittels Telefoninterviews vertiefend untersucht (siehe Abschnitt 7.5). Darüber hinaus werden aus den 129 Unternehmen vier Unternehmen ausgewählt, die besonders positive Ausprägungen in Bezug auf

die vier abhängigen Konzepte aufweisen, um ebenfalls auf der Basis von Telefoninterviews zu identifizieren, auf welche Einflussfaktoren diese Ausprägungen zurückzuführen sind.

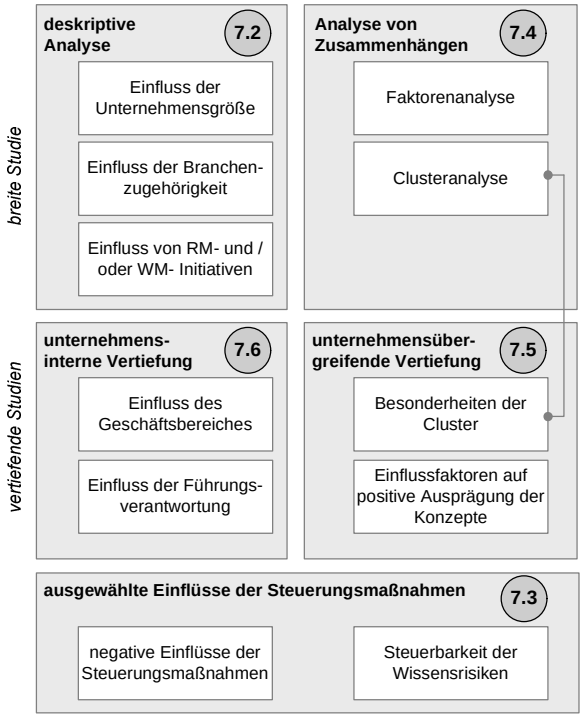


Abb. 32 Auswertungskonzept

Neben der vertieften unternehmensübergreifenden Analyse wird zudem ein Unternehmen der breiten Studie im Hinblick auf die unternehmensinternen Besonderheiten der Steuerung von Wissensrisiken analysiert (siehe Abschnitt 7.6). Die Analyse zielt dabei auf die unterschiedliche Einschätzung über Geschäftsbereiche und Mitarbeitergruppen hinweg ab. Zu diesem Zweck wird eine nach Geschäftsbereichen und Führungsverantwortung geschichtete Stichprobe herangezogen und auf dieser Basis der Fragebogen breit eingesetzt. Analog zur deskriptiven Analyse werden die quantitativen Ergebnisse um qualitative Aspekte, die sich aus der Beantwortung des Interviewleitfadens ergeben, ergänzt. Der in den Abschnitten 5.10.2-5.10.4 auf Basis der Theorie erarbeitete Katalog an Steuerungsmaßnahmen wird in Abschnitt 7.7 vor den Ergebnissen der empirischen Studie reflektiert, um Ergebnisse zu zusätzlichen und Varianten zu bestehenden Steuerungsmaßnahmen zu identifizieren. Das Kapitel schließt mit einer Zusammenfassung und Diskussion (siehe Abschnitt 7.8).
Bevor eine detaillierte Betrachtung der einzelnen Teilstudien erfolgt, werden im nachfolgenden Abschnitt (7.1) Details zur Stichprobe wie die Zusammensetzung der Ansprechpartner und deren Berufserfahrung im Unternehmen und weitere Kennzahlen zur Stichprobe, wie z.B. die Rücklaufquote, dargelegt, um aufzuzeigen vor welchem Hintergrund die Ergebnisse zu interpretieren sind.

7.1 Stichprobenstatistik

Ausgehend von der in Abschnitt 6.3.3 dargestellten Schichtung der Stichprobe nach Branchen und Größenklassen wurden nach dem entsprechenden Ziehungsmuster aus der Adressdatenbank der Creditreform 1290 Adressen in eine Adresskartei überführt, wobei jede Kategorie die zehnfache Anzahl erforderlicher Unternehmen umfasste, da mit einer Rücklaufquote von 10% kalkuliert wurde. Bedingt dadurch, dass der Rücklauf in einigen Branchen schlechter war, erfolgte eine Nachziehung von insgesamt 530 Adressen, wobei in der Baubranche (WZ-F) und im Gastgewerbe (WZ-G)[278] mit 120 und 110 Adressen vergleichsweise umfassende Nachziehungen erfolgten. Somit waren insgesamt 1820

[278] Für eine Übersicht zu den Wirtschaftsabschnitten siehe Tab. 24 in Abschnitt 6.3.3.

Unternehmensadressen Bestandteil der Adresskartei. Von diesen 1820 Unternehmensdressen wurden insgesamt 1216 Adressen genutzt und die Unternehmen nach dem in Abschnitt 6.3.4 beschriebenen Vorgehen kontaktiert.

Studiendetails	**Anzahl / Quote**	
Adressen gesamt	1820	
Unternehmen kontaktiert	1216	
Interviewleitfäden versandt	872	
Versandquote	71,71%	
Rücklauf gesamt	148	
Rücklaufquote	12,17%	
Rücklaufquote nach Branchen	C-F	G-O
	13,79%	10,73%
	Min	Max
	7,06% (H)	18,75% (J)
Rücklaufquote nach Unternehmens-größe	1-9 MA	10-49 MA
	11,63%	20,83%
	50-249 MA	>250 MA
	11,21%	13,30%

Tab. 29 Statistik zum Rücklauf

In 872 Fällen wurden an die jeweiligen Ansprechpartner in den Unternehmen Interviewleitfäden versandt (siehe Tab. 29). Dies entspricht einer Versandquote von 71,71%. Von diesen 872 Interviewleitfäden wurden 37 per Brief (4,24%), 194 per Fax (22,25%) und 641 per E-Mail (73,51%) versandt (siehe Abb. 33). Von den 872 versandten Interviewleitfäden wurden insgesamt 148 beantwortet, was einer Rücklaufquote von 12,17% entspricht. Betrachtet man die Unterschiede zwischen den Branchen, so ist diese im Gastgewerbe (WZ-H) mit 7,06% am geringsten, während sie im Kredit- und Versicherungsgewerbe (WZ-J) mit 18,75% am höchsten ist. Reflektiert man die Rücklaufquote aggregiert über die betrachteten Branchen und fasst die Wirtschaftsabschnitte C-F zur Kategorie produzierende Unternehmen und G-O zu dienstleistungsorientierten Unternehmen zusammen, so liegt die Rücklaufquote bei erstgenannten mit 13,79% vergleichsweise höher als bei dienstleistungsorientierten Unternehmen, die eine Rücklaufquote von 10,73% aufweisen (siehe auch Tab. 29). Im Hinblick auf die Unternehmensgröße variieren die Rücklaufquoten zwischen 11,21% im Falle mittlerer Unternehmen (50-249 Mitarbeiter) bis 20,83% bei Kleinunternehmen (10-49 Mitarbeiter).

Ausgehend von der Schichtung und der korrespondierenden Zielstichprobe von 129 Unternehmen wurden 19 Interviewleitfäden ausgeschlossen, wobei neben der Vollständigkeit der Beantwortung der 36 Aussagen zu den Konzepten die primären Ausschlusskriterien die Besetzung der Kategorien und das Rücklaufdatum waren. Im Hinblick auf das Rücklaufmedium wurden 17 Telefoninterviews (13,18%) geführt und schriftlich fünf Interviewleitfäden per Brief (3,88%), 29 per Fax (22,48%) und 78 per E-Mail (60,74%) beantwortet. Der Anteil der verschiedenen Versand- und Rücklaufmedien ist nochmals in Abb. 33 zusammengefasst.

Im Hinblick auf die in Abschnitt 6.2 definierten Ansprechpartner ergab sich folgende Zusammensetzung. Von den 129 in der Stichprobe eingeschlossenen Unternehmen erfolgte in 127 Fällen die Nennung der Stellenbezeichnung. Insgesamt wurden 69 Interviewleitfäden (53,49%) von Ansprechpartnern der Gruppe Geschäftsführung ausgefüllt. Dabei wurden je nach Branche die Stellenbezeichnungen Geschäftsführer, Vorstand, Werksleiter, Heimleiter und kaufmännischer Leiter dieser Gruppe zugeordnet. In 14 Fällen (10,85%) wurde der Interviewleitfaden von der Assisistenz der Geschäftsfüh-

rung oder von Vorstandsassistenten bearbeitet. 26 Interviewleitfäden (20,16%) wurden von leitenden Angestellten ausgefüllt.

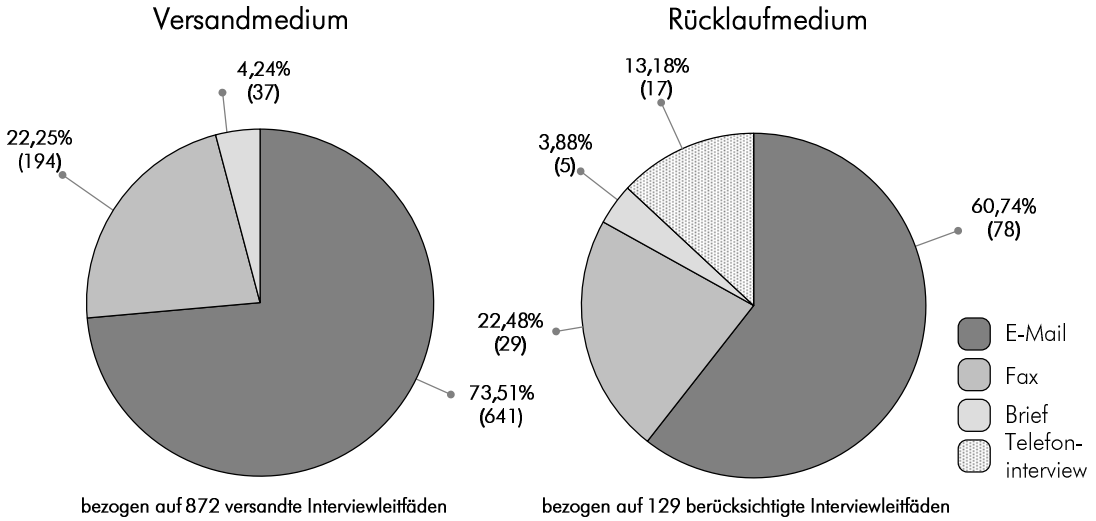


Abb. 33 Versand- und Rücklaufmedien

In dieser Gruppe wurden z.B. Personalleiter, Leiter Organisation, Leiter IT, Pflegedienstleitungen und Prokuristen subsumiert. Ferner wurde der Interviewleitfaden von sieben Mitarbeitern (5,43%) der Unternehmenskommunikation einschließlich zwei Leitern der Abteilung bearbeitet. 11 Interviewleitfäden (8,53%) wurden von Mitarbeitern anderer Stellenbezeichnungen bearbeitet. Diese Gruppe schließt u.a. vier Mitarbeiter im Qualitätsmanagement, Projektleiter und Buchhalter ein. Diese Verteilung ist in Abb. 34 zusammengefasst, wobei die zwei Fragebögen ohne Nennung eines Ansprechpartners 1,55% ausmachen.

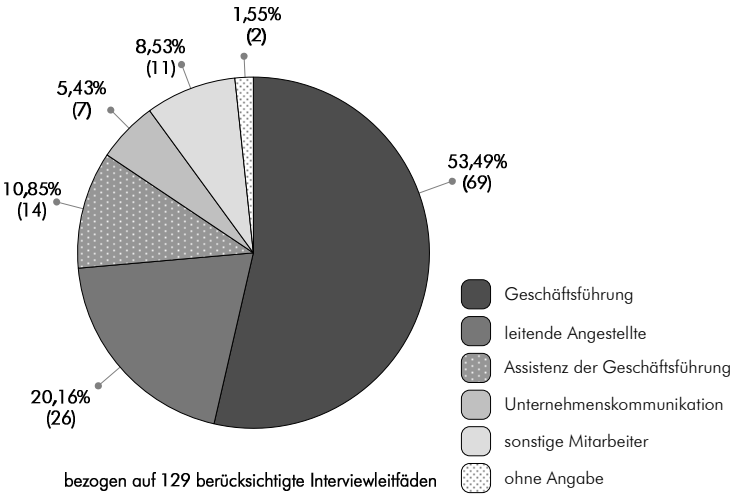


Abb. 34Zusammensetzung der Ansprechpartner

Fasst man die drei Gruppen Geschäftsführung, leitende Angestellte und Assistenz der Geschäftsführung zusammen, so wurde der Interviewleitfaden in 84,5% der Fälle durch die Mitarbeiter der Unternehmenssteuerung im weiten Sinne bearbeitet. Auch die Mitarbeiter der Unternehmenskommunikation passen in die definierte Zielgruppe. Die 11 Ansprechpartner der Gruppe sonstige Mitarbeiter schließen vier Qualitätsmanagementbeauftragte, drei Projektleiter sowie je einen leitenden

Berater, Verwaltungsmitarbeiter, Disponenten und Buchhalter ein. Von diesen 11 Mitarbeitern passen insbesondere die Qualitätsmanagementbeauftragten in das Anforderungsprofil, da dieser Themenkomplex Schnittstellen zum RM und zum Konzept Wissensqualität aufweist.
Im Hinblick auf die Berufserfahrung der Mitarbeiter erfolgte in 120 der 129 berücksichtigten Interviewleitfäden eine Angabe. Dabei ergab sich ein Mittelwert von 11,12 Jahren Berufserfahrung im Unternehmen, wobei als Minimum ein Jahr und als Maximum 41 Jahre genannt wurden. Sieben Ansprechpartner gaben eine Berufserfahrung von einem bzw. 1,5 Jahren im Unternehmen an, während 11 Mitarbeiter zwischen zwei und 2,5 Jahren Berufserfahrung im Unternehmen aufweisen. Somit verfügen 84,17% der Ansprechpartner über eine Berufserfahrung von drei oder mehr Jahren.
Diese hohe durchschnittliche Berufserfahrung im Unternehmen in Kombination mit der ausgeprägten Leitungsfokussierung der Ansprechpartner legt nahe, dass die in den Interviewleitfäden gemachten Angaben eine hohe Qualität aufweisen.

7.2 Deskriptive Analyse der unternehmensübergreifenden Studie

Im folgenden Abschnitt werden auf der Ebene der untersuchten Konzepte die zu dessen Messung herangezogenen Variablen deskriptiv analysiert und Unterschiede zwischen den Teilstichproben mittels induktiver Statistik überprüft. Dazu wird zunächst die Verteilung der entsprechenden Variablen im Hinblick auf die verschiedenen Antwortmöglichkeiten unter Angabe der relevanten Lageparameter dargelegt und interpretiert. Zum Zweiten erfolgt eine Betrachtung der Variablen im Kontext der unterschiedlichen Unternehmensgrößen, die sich aus der Schichtung der Stichprobe nach der Zahl der Mitarbeiter ergibt. Danach werden die Ergebnisse mit der Zugehörigkeit zu verschiedenen Branchen in Beziehung gesetzt. Dabei erfolgt zudem eine Zusammenfassung der 12 eingeschlossenen Wirtschaftsabschnitte zu den beiden Kategorien produzierende (C-F) und dienstleistungsorientierte Unternehmen (G-O), da aufgrund der Schichtungsmerkmale der Umfang der Teilstichproben in einigen Kategorien sehr gering ist und somit die Interpretationen auf Ebene von einzelnen Branchen zum Teil keine statistische Repräsentativität aufweisen. Zudem wird der Einfluss von implementierten RM- und WM-Initiativen auf der Basis entsprechender Teilstichproben analysiert. Zur Analyse des Einflusses werden zwischen den Teilstichproben Mittelwertvergleiche durchgeführt, wobei deren Signifikanz mittels T-Tests[279] überprüft wird. Allgemein wird ein Signifikanzniveau von $\alpha \leq 0{,}05$ festgelegt. Dadurch bedingt, dass diese Mittelwertvergleiche zum Teil über mehrere Variablen eines Konzeptes simultan durchgeführt werden, kann das Problem einer Alphafehler-Kumulierung auftreten, was bedeutet, dass bei einem gleichzeitigen Testen von mehreren Hypothesen einige dieser Hypothesen zufällig signifikant sind. Aus diesem Grund eignet sich die Anwendung eines globalen Signifikanzniveaus nicht in allen Fällen. Stattdessen wird eine Alphafehler-Korrektur vorgenommen, nach der das Signifikanzni-

[279] Für Details siehe hierzu (Hamerle 1996, 33ff).

veau in Abhängigkeit der Anzahl simultan durchgeführter Tests angepasst wird. Für eine derartige Adjustierung bestehen verschiedene Verfahren, wobei die Bonferroni-Korrektur die klassische Anpassung darstellt. Demnach wird das adjustierte Signifikanzniveau als $\alpha^* = \alpha/k$ berechnet, wobei k die Anzahl der simultanen Tests bezeichnet. Diese vergleichsweise strenge und konservative Alphafehler-Korrektur weist insbesondere dann Nachteile auf, wenn mehr als fünf multiple Tests durchgeführt werden (Bender, Lange 2001, 345). Da dies auf den Untersuchungsgegenstand zutrifft, eignen sich als alternative Verfahren für derartige Testsituationen beispielsweise die entsprechenden Korrekturen nach Bonferroni-Holm oder Cross und Chaffin (Bortz, Lienert 2000, 48ff), wobei erstgenannte Korrektur für die nachfolgende Adjustierung der Signifikanzniveaus herangezogen wird. Dabei wird ein globales Signifikanzniveau $\alpha \leq 0{,}1$ zugrunde gelegt, die k Einzeltests durchgeführt und die entsprechenden p-Werte ermittelt. Daraufhin werden die ermittelten p-Werte aufsteigend vom kleinsten zum größten Wert sortiert. Ausgehend vom globalen Signifikanzniveau werden je Test die lokalen Signifikanzniveaus bestimmt. Dabei wird für den ersten Einzeltest das Signifikanzniveau analog Bonferroni als $\alpha^* = \alpha/k$ bestimmt, wobei für den Test mit dem zweitniedrigsten p-Wert das Signifikanzniveau als $\alpha^* = \alpha/(k-1)$ angepasst wird. Für den i-ten Einzeltest gilt somit $\alpha^* = \alpha/(k-i+1)$ (Holm 1979, 65ff). Die Einzeltests sind dann signifikant, wenn der jeweilige p-Wert kleiner als das jeweils adjustierte α^* ist. Für die nachfolgenden Auswertungen wird in Abhängigkeit der Zahl der Einzeltests ein derartiges Vorgehen zugrunde gelegt.

7.2.1 Steuerung von Wissensrisiken

Im folgenden Abschnitt werden die Ergebnisse der breiten Studie im Hinblick auf das Konzept Steuerung von Wissensrisiken erörtert. Dazu werden das arithmetische Mittel (x), das nachfolgend als Mittelwert bezeichnet wird, und der Median (x_{MED}) als Lageparameter sowie die Standardabweichung (σ) als Streuungsmaß angeführt. In Tab. 30 sind diese Parameter in Bezug auf die in Abschnitt 6.3.2 dargelegten Variablen, die das Konzept Steuerung von Wissensrisiken messen, zusammengefasst. Dabei wird der Mittelwert als Ordnungskriterium herangezogen. Alle Variablen sind positiv formuliert und geben den jeweiligen Grad der Implementierung der entsprechenden Steuerungsmaßnahme im betrachteten Unternehmen an. Die Aussagen zu den Variablen sind stark formuliert, d.h. es werden je Aussage Superlative oder verstärkende Wörter wie umfassend etc. verwendet. Zudem sind die Aussagen gemäß der Likert Skala kodiert, wobei 7 mit „ich stimme stark zu“ und 1 mit „ich stimme nicht zu“ belegt ist. Die entsprechende Verteilung je Variable ist ebenfalls in Tab. 30 als absolute Anzahl der Zustimmungen abgetragen.

Entsprechend der Ordnung der Tabelle nach der Höhe des Mittelwertes werden IT-Sicherheitsrichtlinien in Unternehmen im Mittel am umfassendsten eingesetzt (4,81) und auch durch die Mitarbeiter gewissenhaft umgesetzt (4,79). Die vergleichsweise starke Implementierung kann auf

der Basis qualitativer Aussagen aus den Telefoninterviews darauf zurückgeführt werden, dass bedingt durch zahlreiche Standards zum IT-Sicherheitsmanagement und entsprechenden Zertifizierungen dieser Steuerungsmaßnahme eine hohe Bedeutung beigemessen wird. Zu nennen sind in diesem Bereich die weit verbreiteten IT-Grundschutzkataloge, in denen entsprechende Empfehlungen ausgesprochen werden[280]. Auch einer gewissenhaften Umsetzung der Sicherheitsmaßnahmen durch die Mitarbeiter wird vergleichsweise stark zugestimmt. Ein enger Zusammenhang zwischen diesen beiden Variablen zeigt sich dabei durch die vergleichsweise hohe Korrelation[281] von 0,62. Problematisch sind in Bezug auf diese Variable die in Abschnitt 6.3.2 thematisierten Aspekte der Beobachtbarkeit und der Antwortbereitschaft bzw. -verfälschung. So waren sich einige Ansprechpartner bei Telefoninterviews nicht sicher, ob die Umsetzung entsprechend gewissenhaft erfolgt oder nicht und vermuteten dies nur. Neben IT-Sicherheitsrichtlinien und deren Umsetzung sind auch Geheimhaltungsvereinbarungen, die vielfach Teil der Arbeitsverträge sind, als Steuerungsmaßnahme zur Kontrolle der unerwünschten Diffusion von Wissen an externe Dritte im Mittel vergleichsweise umfassend implementiert, was sich auch in einem Mittelwert von 4,77 zeigt. In Bezug auf die Verteilung in Tab. 30 fällt bei dieser Variable auf, dass 49,61% der Befragten mit 6 oder 7 zustimmen. Die Bedeutung dieser Steuerungsmaßnahme hat sich zudem bei der Beantwortung der offenen Fragen zur Priorisierung der 13 Steuerungsmaßnahmen gezeigt[282]. Neben diesen drei umfassend implementierten Steuerungsmaßnahmen werden Kooperationsvereinbarungen, Konkurrenzschutzklauseln und gewerbliche Schutzrechte vergleichsweise weniger in den untersuchten Unternehmen umgesetzt. Der Mittelwert von 3,36 im Falle von Kooperationsvereinbarungen, die zugleich mit 2,05 die höchste Standardabweichung aufweisen, kann durch die Beobachtung, dass 41,09% der befragten Unternehmen dem Einsatz derartiger Vereinbarungen nicht oder nur gering zugestimmt haben, gestützt werden. Dies kann eventuell darauf zurückgeführt werden, dass diese Unternehmen nicht über Kooperationsbeziehungen verfügen bzw. diesen eine geringe Bedeutung beimessen. Neben Kooperationsvereinbarungen werden auch Konkurrenzschutzklausel in geringerem Umfang in den betrachteten Unternehmen eingesetzt, was sich in einem Mittelwert von 3,57 niederschlägt. Basierend auf qualitativen Ergänzungen in den Telefoninterviews ist die vergleichsweise geringe Implementierung dadurch zu erklären, dass laut Aussage einiger Interviewpartner derartige Klauseln vorwiegend bei Führungskräften bzw. Spezialisten eingesetzt werden. Da die Gruppe der betroffenen Mitarbeiter eingeschränkt ist, nivelliert sich auch der korrespondierende Wert, da die entsprechende Aussage auf einen umfassenden Einsatz ausgerichtet ist. Bei einem

[280] Zu den IT-Grundschutzkatalogen siehe auch Abschnitt 4.4.2.

[281] Die Korrelation wurde mittels des Korrelationskoeffizienten nach Bravais Pearson ermittelt und kann auch der Tab. 95 im Anhang A 4 entnommen werden.

[282] Geheimhaltungsvereinbarungen wurden in Bezug auf die offene Frage zur Priorisierung der Steuerungsmaßnahmen mit zehn Nennungen am dritthäufigsten genannt. Siehe hierzu auch Tab. 35 auf Seite 286.

eingeschränkten Mitarbeiterkreis, kann allerdings kein umfassender Einsatz erwartet werden. Die Ergebnisse dürften somit mit der Gruppenzugehörigkeit der Mitarbeiter variieren[283].

Auch gewerbliche Schutzrechte werden in einem vergleichsweise geringeren Umfang eingesetzt und weisen einen Mittelwert von 3,65 auf. Auch in diesem Fall soll das Ergebnis vor dem Hintergrund der Existenz verschiedener Gruppen betrachtet werden. Diese Unterschiede werden nachfolgend im Detail bei der Thematisierung des Einflusses der Branchenzugehörigkeit erläutert, da vermutet werden kann, dass gewerbliche Schutzrechte wie Patente v.a. in produzierenden Unternehmen umfassender eingesetzt werden bzw. eine höhere Bedeutung aufweisen.

n=129				**Wert der Likert Skala**						
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
IT-Sicherheitsrichtlinien	4,81	5	1,81	22	42	13	19	13	14	6
IT-Sicherheitsbewusstsein	4,79	5	1,42	10	36	37	23	11	10	2
Geheimhaltungsvereinbarungen	4,77	5	1,81	20	44	12	18	17	10	8
Dynamisierung der Zugriffsrechte	4,51	5	1,57	8	35	27	26	17	10	6
Klassifikation von Wissen	4,50	5	1,76	15	32	23	24	9	20	6
Zutrittsbeschränkung	4,46	5	1,72	14	29	24	27	13	14	8
Zugriffsbeschränkung	4,42	4	1,74	14	30	20	28	13	17	7
Wissenstransferrichtlinien	4,33	5	1,86	14	32	19	20	17	15	12
Begrenzung der Interaktion	4,32	5	1,79	9	32	29	20	13	12	14
Redundanzschaffung	3,90	4	1,72	5	24	24	22	20	22	12
gewerbliche Schutzrechte (IP)	3,65	4	1,98	9	24	14	20	15	22	25
Konkurrenzschutzklauseln	3,57	3	1,95	8	20	19	17	17	22	26
Kooperationsvereinbarungen	3,36	3	2,05	13	14	12	17	20	18	35

Tab. 30 Verteilung und Lageparameter zum Konzept Steuerung von Wissensrisiken

Zwischen diesen Steuerungsmaßnahmen, die entweder umfassender oder in geringerem Umfang in den betrachteten Unternehmen eingesetzt werden, bestehen weitere Steuerungsmaßnahmen, die eher um die in der Skala definierte Mitte verteilt sind und daher nicht explizit interpretiert werden. Neben der allgemeinen Betrachtung der Mittelwerte, Streuung und Verteilung der verschiedenen Variablen zum Konzept Steuerung von Wissensrisiken sollen nachfolgend speziell Unterschiede identifiziert werden, die sich auf die Unternehmensgröße zurückführen lassen. In Tab. 31 sind die Mittelwerte der Variablen des Konzeptes Steuerung von Wissensrisiken im Kontext der verschiedenen Unternehmensgrößen abgetragen. Im Kontext dieser Studie sind insbesondere Unterschiede zwischen Groß- und mittleren Unternehmen von Relevanz und folglich die Differenz der Mittelwerte als entsprechende Spalte in Tab. 31 berücksichtigt. Diese Differenz wird zugleich als Ordnungskriterium herangezogen und demzufolge die Steuerungsmaßnahmen entsprechend der größten Abweichung zwischen Groß- und mittleren Unternehmen sortiert. Unabhängig von dieser Sortierung ist erkennbar, dass Steuerungsmaßnahmen durchgängig bis auf die Klassifikation von Wissen (-0,01) in Großunternehmen umfassender implementiert sind.

[283] Diese Aspekte werden in der unternehmensinternen vertiefenden Studie genauer betrachtet. Siehe hierzu Abschnitt 7.6.

		Mitarbeiterzahl				
		a	b	c	d	
	n=129	n=12	n=12	n=83	n=22	Δ
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
IT-Sicherheitsrichtlinien	4,81	3,42	4,58	4,80	5,73	0,93
Wissenstransferrichtlinien	4,33	4,58	4,33	4,11	5,00	0,89
Zutrittsbeschränkung	4,46	4,33	4,50	4,29	5,14	0,85
gewerbliche Schutzrechte (IP)	3,65	3,33	3,83	3,51	4,27	0,77
Zugriffsbeschränkung	4,42	4,17	4,00	4,36	5,00	0,64
Geheimhaltungsvereinbarungen	4,77	4,25	4,25	4,78	5,27	0,49
IT-Sicherheitsbewusstsein	4,79	4,08	4,83	4,78	5,18	0,40
Dynamisierung der Zugriffsrechte	4,51	4,33	3,58	4,57	4,91	0,34
Begrenzung der Interaktion	4,32	4,50	4,25	4,24	4,55	0,30
Kooperationsvereinbarungen	3,36	4,08	3,17	3,24	3,55	0,30
Konkurrenzschutzklauseln	3,57	3,92	3,42	3,49	3,73	0,23
Redundanzschaffung	3,90	4,25	3,58	3,87	4,00	0,13
Klassifikation von Wissen	4,50	4,83	3,75	4,55	4,55	-0,01

Tab. 31 Steuerung von Wissensrisiken im Kontext der Unternehmensgröße

Dabei nehmen die Mittelwerte im Falle von IT-Sicherheitsrichtlinien mit 5,73, Geheimhaltungsvereinbarungen mit 5,27 und das IT-Sicherheitsbewusstsein der Mitarbeiter mit 5,18 in Großunternehmen hohe Werte an. Diese Abweichungen zwischen den beiden Unternehmensgrößenklassen sind unter Zugrundlegung von T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}0077$[284] allerdings in keinem Fall signifikant.

Nachdem der Einfluss der Unternehmensgröße erläutert wurde wird nachfolgend der Einfluss der Branchenzugehörigkeit auf die Variablen des Konzeptes Steuerung von Wissensrisiken analysiert. Dabei werden wie in Tab. 32 dargestellt die Branchen C-F zu produzierenden (n=50) und die Branchen G-O zu dienstleistungsorientierten Unternehmen (n=79) zusammengefasst. Zur Sortierung der Tabelle wird als Ordnungskriterium die betragsmäßige Differenz der Mittelwerte zwischen produzierenden und dienstleistungsorientierten Unternehmen herangezogen. Zusätzlich ist je Steuerungsmaßnahme das jeweilige Minimum und Maximum des Mittelwertes über alle 12 Branchen hinweg abgetragen und soll einen groben Anhaltspunkt zur Spannweite der Variablen liefern. Insgesamt werden bei einer groben Betrachtung in produzierenden Unternehmen Steuerungsmaßnahmen vergleichsweise umfassender implementiert, was sich darin zeigt, dass zehn der 13 Steuerungsmaßnahmen in dieser Teilstichprobe einen höheren Mittelwert aufweisen. Die stärkste Abweichung der Mittelwerte besteht in Bezug auf den Einsatz gewerblicher Schutzrechte wie Patente. In diesem Fall ergibt sich eine Mittelwertabweichung von 1,03 zugunsten produzierender Unternehmen. Die Abweichung ist bei Zugrundelegung eines adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}0077$ als einzige Variable signifikant. Dies ist dadurch zu erklären, dass die Patentierbarkeit von Produkten zwischen diesen beiden Teilstichproben variiert. So sind beispielsweise Erfindungen, die sich auf eine technische Entwicklung, wie z.B. ein innovatives physisches Produkt oder ein Fertigungsverfahren, insbesondere im verarbeitenden Gewerbe (WZ-D) verbreitet, während in dienstleistungsorientierten Unternehmen, die eher

[284] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/13 = 0{,}0077$.

immaterielle Produkte erstellen, die Voraussetzungen für eine Patentierbarkeit[285] vielfach gar nicht gegeben sind.

Branchenzugehörigkeit n=129				a n=50	b n=79	Δ
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
gewerbliche Schutzrechte (IP)	2,00	3,65	4,53	4,28	3,25	1,03*
Konkurrenzschutzklauseln	2,40	3,57	4,33	3,76	3,44	0,32
Redundanzschaffung	3,00	3,90	4,63	4,08	3,78	0,30
Kooperationsvereinbarungen	1,60	3,36	4,50	3,52	3,27	0,25
IT-Sicherheitsrichtlinien	3,60	4,81	5,20	4,96	4,71	0,25
Begrenzung der Interaktion	2,80	4,32	5,25	4,46	4,23	0,23
Geheimhaltungsvereinbarungen	3,00	4,77	5,60	4,90	4,68	0,22
Dynamisierung der Zugriffsrechte	3,40	4,51	5,29	4,40	4,58	-0,18
Zugriffsbeschränkung	3,13	4,42	5,25	4,52	4,35	0,17
IT-Sicherheitsbewusstsein	3,40	4,79	5,75	4,88	4,73	0,15
Klassifikation von Wissen	3,60	4,50	5,80	4,58	4,46	0,12
Wissenstransferrichtlinien	3,38	4,33	5,50	4,28	4,35	-0,07
Zutrittsbeschränkung	3,75	4,46	6,00	4,44	4,47	-0,03

Tab. 32 Steuerung von Wissensrisiken im Kontext der Branchenzugehörigkeit

Nachdem größen- und branchenbedingte Unterschiede aufgezeigt wurden, wird nachfolgend der Einfluss von WM- und RM-Initiativen analysiert. Dabei wird eine Aufteilung in mehrere Teilstichproben, die sich im Hinblick auf die Implementierung von WM- und RM-Initiativen unterscheiden, vorgenommen und für diese Gruppen der jeweilige Mittelwert abgetragen. Dabei werden als Teilstichproben Unternehmen zusammengefasst, die weder WM- noch RM- (n=50), nur WM- (n=11), nur RM- (n=29) oder sowohl WM- als auch RM-Initiativen (n=40) implementiert haben. Den Fokus der Betrachtung bilden dabei diejenigen Unternehmen, die in beiden Bereichen entsprechende Maßnahmen einsetzen, da vermutet wird, dass gerade diese Unternehmen ein besonders hohes Bewusstsein für Wissensrisiken aufweisen. Diese Unternehmen werden durch die Bildung von Mittelwertdifferenzen einerseits mit Unternehmen in Beziehung gesetzt, die in keinem der beiden Bereiche Maßnahmen implementiert haben und andererseits mit Unternehmen, die nur in einem der beiden Bereiche über Initiativen verfügen. Als primäres Ordnungskriterium wird in Tab. 33 erstgenannte Differenz herangezogen, wobei die Sortierung absteigend erfolgt. In Bezug auf die Abweichung wird aus Tab. 33 ersichtlich, dass in Unternehmen mit Maßahmen zu RM und WM im Vergleich zu Unternehmen ohne Initiativen in diesen beiden Bereichen alle 13 Steuerungsmaßnahmen einen höheren Mittelwert aufweisen, was einen höheren Steuerungsgrad in dieser Teilstichprobe impliziert. Für diese Differenzen wurde wie in den vorangegangenen Fällen das adjustierte Signifikanzniveau von $\alpha^* \leq 0{,}0077$ zugrunde gelegt. Demnach weichen die Variablen gewerbliche Schutzrechte, Klassifikation von Wissen, Wissenstransferrichtlinien, IT-Sicherheitsrichtlinien, Dynamisierung der Zugriffsrechte, Konkurrenzschutzklauseln, Geheimhaltungsvereinbarungen und Redundanzschaffung positiv ab und sind somit in Unternehmen, die Maßnahmen in beiden Bereichen im Vergleich zu Unternehmen mit Maßnahmen in keinem Bereich

[285] Siehe hierzu auch SR6 in Abschnitt 5.10.4.

stärker implementiert. Somit ist davon auszugehen, dass die Implementierung von Maßnahmen in beiden Bereichen die Steuerungsintensität erhöht.

RM und WM								
		a	b	c	d			
	n=129	n=50	n=11	n=28	n=40	Δ	Δ	Δ
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
gewerbliche Schutzrechte (IP)	3,65	3,08	3,55	3,36	4,60	1,24	1,05	1,52*
Klassifikation von Wissen	4,50	3,90	4,09	4,46	5,40	0,94	1,31	1,50*
Wissenstransferrichtlinien	4,33	3,74	4,45	4,04	5,23	1,19	0,78	1,49*
IT-Sicherheitsrichtlinien	4,81	4,06	4,45	5,46	5,38	-0,08	0,93	1,32*
Dynamisierung der Zugriffsrechte	4,51	3,86	4,36	4,93	5,08	0,15	0,72	1,22*
Konkurrenzschutzklauseln	3,57	3,04	3,18	3,75	4,20	0,45	1,02	1,16*
Geheimhaltungsvereinbarungen	4,77	4,24	4,73	4,86	5,38	0,52	0,65	1,14*
Redundanzschaffung	3,90	3,40	3,82	3,93	4,53	0,6	0,71	1,13*
IT-Sicherheitsbewusstsein	4,79	4,18	4,91	5,32	5,15	-0,17	0,24	0,97*
Kooperationsvereinbarungen	3,36	3,14	3,45	2,89	3,95	1,06	0,5	0,81
Begrenzung der Interaktion	4,32	4,06	4,18	4,39	4,63	0,24	0,45	0,57
Zugriffsbeschränkung	4,42	4,12	4,64	4,57	4,63	0,06	-0,01	0,51
Zutrittsbeschränkung	4,46	4,36	3,64	4,61	4,70	0,09	1,06	0,34

Tab. 33 Steuerung von Wissensrisiken im Kontext von RM- und WM-Initiativen

Die Mittelwertvergleiche zwischen den anderen Gruppen sind bei analogem Signifikanzniveau in keinem Fall signifikant.

Diese Abweichung und somit der Einfluss von WM- und RM-Initiativen können weiterhin im Kontext des Zusammenhangs zwischen diesen Initiativen und der Unternehmensgröße sowie Branchenzugehörigkeit reflektiert werden. Betrachtet man die Korrelationen zwischen RM- und WM-Initiativen und diesen beiden Stichprobenmerkmalen so ergeben sich bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}025$[286] die in Tab. 34 dargestellten Zusammenhänge. Demnach implementieren Unternehmen mit steigender Unternehmensgröße umfassender RM-Initiativen. Auch in Bezug auf WM-Initiativen ergibt sich eine positive Korrelation in Bezug auf die Unternehmensgröße, die zugleich den zweithöchsten p-Wert aufweist und somit ebenfalls nach Bonferroni-Holm signifikant ist. In Bezug auf die Branchenzugehörigkeit bestehen keinerlei signifikante Korrelationen. Somit treffen die Abweichungen, die in Zusammenhang mit RM- und WM-Initiativen stehen, insbesondere auf Großunternehmen zu, da diese signifikant umfassender diese Initiativen ergreifen.

		Unternehmens-größe	**Branchen-zugehörigkeit**
RM-Initiativen	Spearmans Rho	0,286	0,018
	Signifikanz	0,001*	0,840
WM-Initiative	Spearmans Rho	0,187	-0,088
	Signifikanz	0,033*	0,322

Tab. 34 Korrelationen im Kontext der RM- und WM-Initiativen

[286] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/(2x2)=0{,}025$.

Zusätzlich zur Zustimmung zu den Aussagen sind in Bezug auf das Konzept Steuerung von Wissensrisiken noch zwei offene Fragen Gegenstand des Interviewleitfadens. Die eine Frage dient dabei zur Priorisierung der im Interviewleitfaden genannten Steuerungsmaßnahmen aus der Perspektive der Ansprechpartner, während die zweite offene Frage die Angabe zusätzlicher relevanter Steuerungsmaßnahmen ermöglichen soll. Die Frage zur Priorisierung der Steuerungsmaßnahmen wurde in 57 Fällen beantwortet, wobei die Zahl der priorisierten Steuerungsmaßnahmen von eins bis vier reicht und im Mittel zwei Steuerungsmaßnahmen angegeben wurden. Mithilfe von Tab. 35 werden die priorisierten Steuerungsmaßnahmen im Hinblick auf die Häufigkeit der Nennung zusammengefasst, wobei nur Steuerungsmaßnahmen eingeschlossen wurden, die in Summe dreimal oder öfter genannt wurden.

Steuerungsmaßnahme	**Anzahl**
Dokumentation	16
Personalentwicklung	11
Geheimhaltungsvereinbarungen	10
Zugriffsbeschränkung	9
Sensibilisierung der Mitarbeiter	7
Zutrittsbeschränkung	6
Nachfolgeplanung	6
IT-Sicherheitsrichtlinien	5
Schaffung von Rollen	5
Reduktion Abhängigkeit	5
Unternehmenskultur	4
Klassifikation von Wissen	4
Wissenstransferrichtlinien	3
Mitarbeiterbindung	3
Kontrolle	3
Wettbewerberbeobachtung	3

Tab. 35 Priorisierung der Maßnahmen

Die Ergebnisse erheben dabei keinen Anspruch auf Repräsentativität, sollen allerdings die quantitativen Ergebnisse um qualitative Aspekte ergänzen und einen Eindruck vermitteln, welche Steuerungsmaßnahmen in Unternehmen als besonders relevant bzw. wirkungsvoll angesehen werden. Die beiden am häufigsten erwähnten Steuerungsmaßnahmen stellen die Dokumentation von Wissen mit 16 und die Personalentwicklung mit 11 Nennungen dar. Basierend auf den Erfahrungen aus den Telefoninterviews wird die Dokumentation insbesondere auch als Maßnahme gesehen, mittels derer Nachfolge- und Vertreterprobleme reduziert werden können. Personalentwicklung ist nicht Gegenstand der zur Operationalisierung des Konzeptes herangezogenen Variablen, scheint allerdings aufgrund der vergleichsweise häufigen Nennung eine gewisse Bedeutung einzunehmen. Im Detail wurde z.B. die Schulung der Mitarbeiter in Bezug auf Sicherheitsmaßnahmen angeführt. Am dritt- und vierthäufigsten wurden Geheimhaltungsvereinbarungen und mit elektronische Zugriffskontrollen mit zehn bzw. neun Nennungen angeführt. Erwähnenswert erscheint ebenso die Sensibilisierung der Mitarbeiter mit sieben Nennungen, die sich zusätzlich durch weitere Maßnahmen wie wissensrisikobewusste Unternehmenskultur (4), Motivation (2) und Führung (1), die ebenfalls eher kulturelle bzw. personalwirtschaftliche Aspekte fokussieren, ergänzt werden kann.

Zusammenfassend betrachtet werden über alle Steuerungsmaßnahmen hinweg IT-Sicherheitsrichtlinien am umfassendsten eingesetzt und auch gewissenhaft durch die Mitarbeiter umgesetzt. Zudem sind auch Geheimhaltungsvereinbarungen vergleichsweise umfassend implementiert. Die Bedeutung letzterer kann zudem durch die vergleichsweise häufige Nennung (10) dieser Maßnahmen hinsichtlich der Frage zur Priorisierung (siehe Tab. 35) unterstrichen werden. Großunterneh-

men weisen im Vergleich zu mittleren Unternehmen höhere Mittelwerte auf, wobei die Differenzen nicht signifikant sind. Im Hinblick auf den Einfluss der Branchenzugehörigkeit und die Zusammenfassung verschiedener Branchen zu produzierenden und zu dienstleistungsorientierten Unternehmen ist nur die Mittelwertdifferenz in Bezug auf die Steuerungsmaßnahme gewerbliche Schutzrechte signifikant, was darauf zurückzuführen ist, dass v.a. Patente in produzierenden Unternehmen eine vergleichsweise höhere Bedeutung aufweisen. Bezüglich des Einflusses von RM- und WM-Initiativen kann als Ergebnis festgehalten werden, dass Unternehmen, die Maßnahmen in beiden Bereichen einsetzen stärker steuern, wobei diese Unterschiede in neun der 13 Fälle auch signifikant sind.

7.2.2 Wissensverlust

Das Konzept Wissensverlust ist negativ operationalisiert, weshalb eine hohe Zustimmung zu den Aussagen auf ein hohes Risiko hindeutet. Eine Ausnahme bilden dabei die beiden Aussagen zur Dokumentation von Wissen, die im Interviewleitfaden (siehe Anhang A 1) positiv formuliert sind. Um die Interpretation auf Konzeptebene auf einer einheitlichen Basis vornehmen zu können, wurden diese beiden Aussagen rekodiert.

n=129				**Wert der Likert Skala**						
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Nichtdokumentation (TG)[287]	3,86	4	1,56	6	14	25	32	24	19	9
Vertretung	3,81	4	1,60	3	23	21	22	27	26	7
Nachbesetzung	3,73	4	1,64	1	23	24	22	21	27	11
Nichtdokumentation (PG) [288]	3,47	3	1,53	2	15	20	17	32	36	7
Reorganisation	3,01	3	1,49	0	9	19	14	26	44	17
Verlust dokumentierten Wissens	2,47	2	1,49	0	9	8	11	15	49	37

Tab. 36 Verteilung und Lageparameter zum Konzept Wissensverlust

In Tab. 36 sind Mittelwert, Median und Standardabweichung ebenso wie die Verteilung der Zustimmung zu den Aussagen abgetragen. Zur Sortierung der Tabelle wird der Mittelwert als Ordnungskriterium herangezogen. Insgesamt liegen alle sechs Variablen unter der durch die Likert Skalierung vorgegebenen Mitte. Entsprechend dieser Ordnung wird das Risiko in Bezug auf eine Nichtdokumentation von Wissen im Tagesgeschäft mit einem Mittelwert von 3,86 am höchsten eingeschätzt. Vertretungs- (3,81) und Nachbesetzungsprobleme (3,73), die sich auf eine unzureichende Rekonstruierbarkeit des Wissens im jeweiligen Fall zurückführen lassen, werden am zweit- bzw. drittstärksten eingeschätzt. Am geringsten wird das Risiko des Verlustes dokumentierten Wissens eingeschätzt. 66,67% der befragten Unternehmen haben der korrespondierenden Aussage nicht oder nur gering zugestimmt. Daher ergibt sich ein vergleichsweise niedriger Mittelwert von 2,47. Ein Grund für diese geringe Ausprägung könnten die umfassend implementierten IT-Sicherheitsrichtlinien bzw. das entsprechend

[287] TG steht für Tagesgeschäft.
[288] PG steht für Projektgeschäft.

hohe IT-Sicherheitsbewusstsein sein, die wie in Abschnitt 7.2.1 erläutert Mittelwerte von 4,81 bzw. 4,79 aufweisen[289].

		Mitarbeiterzahl				
		a	b	c	d	
n=129		n=12	n=12	n=83	n=22	**Δ**
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
Nichtdokumentation (TG)	3,86	4,58	4,17	3,94	3,00	-0,94*
Nichtdokumentation (PG)	3,47	4,17	3,92	3,49	2,73	-0,77*
Verlust dokumentierten Wissens	2,47	2,08	2,67	2,61	2,00	-0,61
Reorganisation	3,01	2,75	3,17	3,12	2,64	-0,48
Vertretung	3,81	3,75	4,33	3,84	3,45	-0,39
Nachbesetzung	3,73	4,08	4,17	3,71	3,36	-0,35

Tab. 37 Wissensverlust im Kontext der Unternehmensgröße

Mithilfe von Tab. 37 werden Unterschiede, die sich potentiell auf die Unternehmensgröße zurückführen lassen, analysiert, wobei wiederum große und mittlere Unternehmen den Hauptuntersuchungsgegenstand darstellen. Tab. 37 ist nach der Höhe der Mittelwertabweichung zwischen diesen beiden Größenklassen sortiert. Insgesamt weisen die 22 Großunternehmen vergleichsweise geringere Mittelwerte in Bezug auf alle sechs Variablen auf, wobei unter Zugrundelegung eines adjustierten Signifikanzniveaus von $\alpha^*=0{,}0167$[290] die beiden Variablen zur Dokumentation im Tages- bzw. Projektgeschäft signifikant sind. Eine Begründung dafür kann nach qualitativen Aussagen darin liegen, dass Dokumentationsprozesse in Großunternehmen vergleichsweise umfassender implementiert sind.

n=129	Branchenzugehörigkeit			a	b	
				n=50	n=79	**Δ**
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
Nachbesetzung	2,00	3,73	4,80	3,98	3,57	0,41
Vertretung	2,86	3,81	5,00	4,06	3,66	0,40
Nichtdokumentation (PG)	2,75	3,47	5,40	4,32	4,67	-0,35
Nichtdokumentation (TG)	3,29	3,86	5,50	3,96	4,25	-0,29
Verlust dokumentierten Wissens	1,75	2,47	3,25	2,58	2,39	0,19
Reorganisation	2,17	3,01	4,50	3,12	2,94	0,18

Tab. 38 Wissensverlust im Kontext der Branchenzugehörigkeit

Nachdem größenbedingte Unterschiede betrachtet wurden, werden basierend auf den in Tab. 38 dargestellten Ergebnissen, Unterschiede erörtert, die im Zusammenhang mit der Branchenzugehörigkeit stehen. Zu diesem Zweck sind in Tab. 38 ausgehend von der Aufteilung der Stichprobe in produzierende und dienstleistungsorientierte Unternehmen die entsprechenden Mittelwerte und die Abweichung zwischen den beiden Gruppen abgetragen. Zusätzlich sind je Variable das jeweilige Minimum und Maximum vermerkt, um die Spannweite aufzuzeigen. Insgesamt zeigt sich, dass die Mittelwerte bei dienstleistungsorientierten Unternehmen durchgängig über alle sechs Variablen niedriger sind und somit auch die korrespondierenden Risiken niedriger eingeschätzt werden. Bei

[289] Betrachtet man die Korrelationen, so ergibt sich in beiden Fällen ein schwach signifikanter Zusammenhang. So beträgt die Korrelation des Verlustes dokumentierten Wissens und IT-Sicherheitsrichtlinien -0,25, während IT-Sicherheitsbewusstsein eine Korrelation -0,24 aufweist.

[290] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/6=0{,}0167$

Überprüfung dieser Abweichungen mittels T-Tests bei einem adjustierten Signifikanzniveaus von $\alpha^*=0{,}0167$ kann allerdings für keine Abweichung Signifikanz nachgewiesen werden.

Nachdem Unterschiede in Bezug auf die Unternehmensgröße und die Branchenzugehörigkeit erörtert wurden, wird nachfolgend der Einfluss von implementierten WM- und RM-Initiativen analysiert und primär Unternehmen betrachtet, die in beiden Bereichen Initiativen einsetzen. Diese Teilstichprobe wird mit Unternehmen, die entweder in einem der beiden Bereiche bzw. in keinem Bereich Maßnahmen implementiert haben, durch die Bildung von Mittelwertabweichungen verglichen, wobei die betragsmäßige Differenz aus letztgenannten auch zugleich das Ordnungskriterium von Tab. 39 darstellt. Insgesamt werden in Unternehmen, die RM- und WM-Maßnahmen implementiert haben, im Vergleich zu Unternehmen ohne Maßnahmen in einem der beiden Bereiche die korrespondierenden Risiken in Bezug auf fünf der sechs Variablen geringer eingeschätzt. Dabei sind die Unterschiede bei Zugrundelegung eines adjustierten Signifikanzniveaus von $\alpha^*=0{,}0167$ in Bezug auf die Variablen Nichtdokumentation im Tages- und Projektgeschäft sowie Verlust dokumentierten Wissens signifikant.

RM und WM								
		a	**b**	**c**	**d**			
	n=129	n=50	n=11	n=28	n=40	**Δ**	**Δ**	**Δ**
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
Nichtdokumentation (TG)	3,86	4,42	3,91	4,00	3,05	-0,95*	-0,86	-1,37*
Nichtdokumentation (PG)	3,47	3,90	3,73	3,43	2,88	-0,55*	-0,85	-1,02*
Verlust dokumentierten Wissens	2,47	2,78	3,18	2,29	2,00	-0,29	-1,18	-0,78*
Reorganisation	3,01	3,28	3,55	2,75	2,70	-0,05	-0,85	-0,58
Vertretung	3,81	3,76	4,55	3,75	3,73	-0,02	-0,82	-0,03
Nachbesetzung	3,73	3,58	4,55	3,82	3,63	-0,19	-0,92	0,05

Tab. 39 Wissensverlust im Kontext von RM- und WM-Initiativen

Weiterhin ergeben sich bei einem Vergleich der Mittelwerte zwischen Unternehmen mit Maßnahmen in beiden Bereichen und Unternehmen, die nur RM-Maßnahmen implementiert haben, bei analogem Signifikanzniveau ebenfalls signifikante Abweichungen in Bezug auf die beiden Variablen zur Nichtdokumentation. In beiden Fällen wird das Risiko einer Nichtdokumentation in Unternehmen, die nur RM-Maßnahmen implementiert haben, signifikant höher bewertet. Dies kann so interpretiert werden, dass WM-Maßnahmen die korrespondierenden Risiken reduzieren[291].

Insgesamt werden alle Variablen zur Operationalisierung des Wissensverlustes vergleichsweise niedrig eingeschätzt und liegen unter der durch die Likert Skala vorgegebenen Mitte. Großunternehmen schätzen im Vergleich zu mittleren Unternehmen, die Risiken geringer ein, wobei die Wissensrisiken im Zusammenhang mit der Nichtdokumentation durch diese Unternehmensgruppe signifikant geringer

[291] Die in dieser Tabelle dargestellten Zusammenhänge sind für Unternehmen mit zunehmender Mitarbeiterzahl von Relevanz, da mit diesem Anstieg sowohl die Implementierung von RM- als auch WM-Initiativen zunimmt (siehe hierzu auch die Korrelationen in Tab. 34 auf Seite 286).

eingeschätzt werden. Auch dienstleistungsorientierte Unternehmen schätzen im Vergleich zu produzierenden Unternehmen Wissensverluste geringer ein, wobei die Abweichungen bezüglich der Branchenzugehörigkeit nicht signifikant sind. Unternehmen, die RM- und WM-Initiativen implementiert haben schätzen in der Relation zu Unternehmen, die Maßnahmen in nur einem oder keinem der beiden Bereiche einsetzen, geringer ein, wobei Signifikanzen zwischen den Teilstichproben zum einen die Variablen zur Nichtdokumentation und zum anderen den Verlust dokumentierten Wissens betreffen.

7.2.3 Wissensdiffusion

Ebenso wie der Wissensverlust ist auch das Konzept Wissensdiffusion negativ gerichtet und folglich ein hoher Wert auf der Likert Skala mit einem hohen Risiko gleichzusetzen. In Tab. 40 sind analog zu den anderen Konzepten Mittelwert, Median, Standardabweichung und die absolute Zahl Zustimmungen abgetragen, wobei die Tabelle nach dem Mittelwert sortiert ist.

n=129				**Wert der Likert Skala**						
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Reverse Engineering	3,86	4	1,96	8	18	24	23	22	22	12
nachteilige Mitarbeiterfluktuation	3,38	3	1,84	7	15	12	22	23	30	20
Imitation	3,14	3	1,77	2	12	13	20	30	32	20
unerwünschter Zugang für Partner	2,57	2	1,60	0	4	11	14	23	51	26
Competitive Intelligence	2,39	2	1,55	0	3	6	15	26	43	36
unautorisierte Zugriffe	2,15	2	1,47	1	2	4	12	18	44	48

Tab. 40 Verteilung und Lageparameter zum Konzept Wissensdiffusion

Insgesamt ist ersichtlich, dass die Mittelwerte aller sechs erhobenen Variablen unter der durch die Likert Skalierung vorgegebenen Mitte liegen und somit die Risiken der Diffusion vergleichsweise gering eingeschätzt werden. Weiterhin sind die drei erstgenannten Wissensrisiken durch eine vergleichsweise hohe Standardabweichung charakterisiert, weshalb die Aussagekraft des Mittelwertes in diesen Fällen reduziert wird. Entsprechend dieser Ordnung wird das Risiko des Reverse Engineering im Vergleich zu den anderen Variablen am höchsten eingeschätzt und weist einen Mittelwert von 3,86 auf. Im Gegensatz dazu wird das Risiko des Auftretens unautorisierter Zugriffe auf elektronisch dokumentiertes Wissen mit einem Mittelwert von 2,15 vergleichsweise gering eingeschätzt, da 71,32% der befragten Unternehmen deren Auftreten vollkommen verneinen oder nur wenig zustimmen. Nach dieser allgemeinen Betrachtung werden mithilfe von Tab. 41 Unterschiede analysiert, die auf die Unternehmensgröße zurückgeführt werden können.

Analog zu den anderen Konzepten wird die absolute Differenz der Mittelwerte zwischen Groß- und mittlere Unternehmen als Ordnungskriterium für Tab. 41 herangezogen und diese beiden Größenklassen fokussiert betrachtet. Insgesamt zeigt sich, dass Wissensrisiken, die die Diffusion betreffen, in Großunternehmen im Vergleich zu mittleren Unternehmen geringer ausgeprägt sind, wobei unter Bezugnahme auf die jeweils errechneten T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}0167$[292] keine der Abweichungen signifikant ist.

		Mitarbeiterzahl				
		a	b	c	d	
	n=129	n=12	n=12	n=83	n=22	**Δ**
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
nachteilige Mitarbeiterfluktuation	3,38	4,25	3,75	3,40	2,64	-0,76
Reverse Engineering	3,86	3,83	3,92	4,00	3,32	-0,68
unerwünschter Zugang für Partner	2,57	2,33	2,92	2,69	2,09	-0,60
Imitation	3,14	2,67	3,58	3,24	2,77	-0,47
unautorisierte Zugriffe	2,15	1,75	2,42	2,23	1,91	-0,32
Competitive Intelligence	2,39	2,08	3,17	2,37	2,18	-0,19

Tab. 41 Wissensdiffusion im Kontext der Unternehmensgröße

Auch die Branchenzugehörigkeit der in der Stichprobe eingeschlossenen Unternehmen hat auf die Variablen der Wissensdiffusion Einfluss. Auf der Basis von Tab. 42 werden nachfolgend die Unterschiede zwischen den Teilstichproben produzierende und dienstleistungsorientierte Unternehmen analysiert und die Mittelwertabweichungen, die auch das Ordnungskriterium darstellen, betrachtet. Zusätzlich sind in Tab. 42 je Variable die Minima und Maxima der Mittelwerte über die verschiedenen Branchen aufgenommen, um die jeweilige Spannweite aufzuzeigen. Hier sei nochmals betont, dass diese Werte nur die Spannweite der Variable aufzeigen sollen und aufgrund des zum Teil geringen Stichprobenumfangs keine statistische Signifikanz gegeben ist. Betrachtet man die Unterschiede zwischen produzierenden und dienstleistungsorientierten Unternehmen, so zeigen die Berechnungen in Tab. 42, dass die Mittelwerte bei produzierenden Unternehmen vergleichsweise höher sind, wobei die Berechnung der T-Tests bei einem adjustierten Signifikanzniveau

	Branchenzugehörigkeit			a	b	
n=129				n=50	n=79	**Δ**
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
unerwünschter Zugang für Partner	1,88	2,57	4,00	2,92	2,35	0,57
Imitation	2,33	3,14	3,63	3,48	2,92	0,56
Reverse Engineering	2,67	3,86	5,40	4,08	3,72	0,36
unautorisierte Zugriffe	1,40	2,15	3,25	2,32	2,04	0,28
nachteilige Mitarbeiterfluktuation	1,50	3,38	4,75	3,46	3,33	0,13
Competitive Intelligence	1,67	2,39	3,50	2,44	2,35	0,09

Tab. 42 Wissensdiffusion im Kontext der Branchenzugehörigkeit

[292] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/6=0{,}0167$.

von $\alpha^*=0{,}0167$[293] zu keinem signifikanten Ergebnis führt. Im Hinblick auf die Minima und Maxima zeigt sich insbesondere bei der Variable nachteilige Mitarbeiterfluktuation eine hohe Spannweite der Mittelwerte von 3,25. Auch die Variable Reverse Engineering ist mit 2,73 durch eine vergleichsweise hohe Spannweite charakterisiert. Mittels Tab. 43 wird der Einfluss von WM- und RM-Initiativen auf das Konzept Wissensdiffusion dargestellt. Den primären Betrachtungspunkt stellen Unternehmen dar, die in beiden Bereichen entsprechende Maßnahmen einsetzen, wobei ausgehend von dieser Teilstichprobe Mittelwertdifferenzen zu Unternehmen mit implementierten Maßnahmen in einem Bereich und zu Unternehmen ohne jegliche Maßnahme gebildet werden. Letztgenannte Differenz stellt dabei das Ordnungskriterium von Tab. 43 dar.

Betrachtet man die Differenzen zwischen den Teilstichproben der Unternehmen mit Maßnahmen in beiden Bereichen und den Unternehmen ohne entsprechende Initiativen, so zeigt sich, dass fünf der sechs Risiken von Unternehmen der erstgenannten Teilstichprobe höher eingeschätzt werden. Diese Abweichungen sind allerdings bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}0167$ nicht signifikant. Analoges trifft auf die beiden anderen Mittelwertvergleiche zu[294].

		RM und WM						
		a	**b**	**c**	**d**			
	n=129	n=50	n=11	n=28	n=40	**Δ**	**Δ**	**Δ**
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
nachteilige Mitarbeiterfluktuation	3,38	3,12	3,82	3,39	3,58	0,19	-0,24	0,46
unautorisierte Zugriffe	2,15	2,12	2,18	1,82	2,40	0,58	0,22	0,28
unerwünschter Zugang für Partner	2,57	2,56	2,55	2,36	2,75	0,39	0,2	0,19
Reverse Engineering	3,86	3,88	3,73	3,71	3,98	0,27	0,25	0,1
Imitation	3,14	3,08	3,09	3,25	3,15	-0,1	0,06	0,07
Competitive Intelligence	2,39	2,48	2,64	2,04	2,45	0,41	-0,19	-0,03

Tab. 43 Wissensdiffusion im Kontext von RM- und WM-Initiativen

Zusammenfassend betrachtet liegen alle Variablen zur Messung des Konzeptes über der durch die Likert Skala vorgegebenen Mitte, wobei dem Risiko Reverse Engineering die höchste und dem Risiko Verlust dokumentierten Wissens die geringste Bedeutung beigemessen wird. Sowohl in Bezug auf die Unternehmensgröße als auch auf die Branchenzugehörigkeit und die Implementierung von RM- und WM-Maßnahmen ergeben sich keinerlei signifikante Unterschiede zwischen den korrespondierenden Teilstichproben.

[293] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/6=0{,}0167$.

[294] Die in dieser Tabelle dargestellten Zusammenhänge sind für Unternehmen mit zunehmender Mitarbeiterzahl von Relevanz, da mit diesem Anstieg sowohl die Implementierung von RM- als auch WM-Initiativen zunimmt (siehe hierzu auch die Korrelationen in Tab. 34 auf Seite 286).

7.2.4 Wissenstransfer

Das Konzept Wissenstransfer ist positiv operationalisiert, weshalb im Gegensatz zu den beiden zuvor erläuterten Konzepten eine hohe Zustimmung zur Aussage und somit ein hoher Wert auf der Likert Skala positiv zu werten ist. Die entsprechende Verteilung des Grades der Zustimmung sowie die Lage- und Streuungsparameter sind über alle 129 Unternehmen in Tab. 44, die absteigend nach dem Mittelwert sortiert ist, abgetragen. Der Beitrag externen Wissens stellt die am höchsten bewertete Variable dar und weist einen Mittelwert von 4,73 auf.

n=129				**Wert der Likert Skala**						
Variable	**x**	$\mathbf{x_{med}}$	**Σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Beitrag externen Wissens	4,73	5	1,84	12	31	30	32	15	8	1
Qualität externen Wissens	4,69	5	1,60	3	36	40	28	13	8	1
Erweiterung der Wissensbasis	4,33	4	1,47	7	25	28	35	14	18	2
Quantität externen Wissens	4,25	4	1,55	3	26	33	29	17	18	3
Reduktion der Abhängigkeit	3,95	4	1,77	6	16	18	45	20	18	6

Tab. 44 Verteilung und Lageparameter zum Konzept Wissenstransfer

Diese Variable ist zudem mit 1,84 durch die höchste Standardabweichung innerhalb des Konzeptes charakterisiert, wodurch die Aussagekraft des Mittelwertes reduziert wird. Am zweithöchsten wird mit einem Mittelwert von 4,69 die Qualität externen Wissens eingeschätzt, während die Reduktion der Abhängigkeiten vom Wissen des Partners als vergleichsweise geringster Erfolgsbeitrag des Wissenstransfers mit durchschnittlich 3,95 bewertet wurde.

		Mitarbeiterzahl				
		a	b	c	d	
	n=129	n=12	n=12	n=83	n=22	**Δ**
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
Qualität externen Wissens	4,69	4,50	4,92	4,53	5,27	0,74*
Quantität externen Wissens	4,25	3,75	4,50	4,12	4,86	0,74*
Erweiterung der Wissensbasis	4,33	4,50	4,08	4,24	4,73	0,49
Beitrag externen Wissens	4,73	5,17	4,67	4,60	5,00	0,40
Reduktion der Abhängigkeit	3,95	3,42	3,67	4,05	4,05	0,00

Tab. 45 Wissenstransfer im Kontext der Unternehmensgröße

Nachfolgend werden Unterschiede der Variablen, die sich auf die Unternehmensgröße zurückführen lassen, analysiert. Dazu sind in Tab. 45 die Mittelwerte der Teilstichproben, die sich aus der Schichtung nach Mitarbeiterzahl ergeben, abgetragen, wobei Groß- und mittleren Unternehmen den primären Betrachtungsgegenstand darstellen. Aus diesem Grund wird ausgehend von Großunternehmen die Mittelwertabweichung für diese beiden Teilstichproben ermittelt und als Sortierungskriterium für Tab. 45 herangezogen. Die Mittelwerte werden in vier der fünf Fälle durch Großunternehmen im Vergleich zu mittelständischen Unternehmen positiver bewertet, wobei auf Basis der T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}02$[295] die Abweichungen in Bezug auf die Variablen Qualität und Quanti-

[295] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/5=0{,}02$

tät dokumentierten Wissens signifikant sind. Zusätzlich zu größenbedingten Unterschieden werden nachfolgend auf der Basis von Tab. 46 branchenbezogene Unterschiede erläutert. Dazu werden als Teilstichproben produzierende und dienstleistungsorientierte Unternehmen betrachtet und je Variable der minimale und maximale Mittelwert über die 12 Branchen hinweg, abgetragen.

n=129	**Branchenzugehörigkeit**			a	b	
				n=50	n=79	**Δ**
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
Reduktion der Abhängigkeit	2,40	3,95	4,83	4,26	3,76	0,50
Quantität externen Wissens	3,40	4,25	5,00	3,98	4,42	-0,44
Erweiterung der Wissensbasis	3,60	4,33	5,00	4,48	4,24	0,24
Qualität externen Wissens	3,40	4,69	5,50	4,58	4,76	-0,18
Beitrag externen Wissens	3,60	4,73	5,50	4,68	4,76	-0,08

Tab. 46 Wissenstransfer im Kontext der Branchenzugehörigkeit

Die teils positiven teils negativen Abweichungen zwischen den Teilstichproben sind bei Zugrundelegung von T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}02$ in keinem Fall signifikant. Neben der Analyse des Einflusses der Unternehmensgröße und der Branchenzugehörigkeit wird mithilfe von Tab. 47 der Einfluss bestehender WM- und RM-Initiativen erörtert, indem die korrespondierenden Teilstichproben untereinander verglichen werden. Als Ordnungskriterium für Tab. 47 wird die Mittelwertabweichung zwischen Unternehmen, die sowohl WM- als auch RM-Initiativen implementiert haben, und Unternehmen, die in keinem der beiden Bereiche Initiativen einsetzen, herangezogen[296].

		RM und WM						
		a	**b**	**c**	**d**			
	n=129	n=50	n=11	n=28	n=40	**Δ**	**Δ**	**Δ**
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
Beitrag externen Wissens	4,73	4,26	4,45	4,68	5,43	0,75	0,98	1,17*
Erweiterung der Wissensbasis	4,33	3,86	4,18	4,29	5,00	0,71	0,82	1,14*
Quantität externen Wissens	4,25	3,92	4,18	4,18	4,73	0,55	0,55	0,81*
Qualität externen Wissens	4,69	4,48	4,27	4,54	5,18	0,64	0,91	0,7*
Reduktion der Abhängigkeit	3,95	3,64	4,36	3,96	4,23	0,27	-0,13	0,59*

Tab. 47 Wissenstransfer im Kontext von RM- und WM-Initiativen

Dabei werden durch Unternehmen, die Initiativen in beiden Bereichen implementiert haben, der Wissenstransfer erfolgreicher bzw. korrespondierende Wissensrisiken geringer eingeschätzt, wobei unter Zugrundelegung entsprechender T-Tests bei einem analogen $\alpha^*=0{,}02$ die Abweichungen bei allen fünf Variablen signifikant sind. Eine Begründung für diese positiven Abweichungen könnte darin liegen, dass Unternehmen, die Maßnahmen in beiden Bereichen implementiert haben, der Dualität des Wissenstransfers bewusst sind. Dies bedeutet, dass diese Unternehmen sich aufgrund der Auseinandersetzung mit WM über den Wert des Wissens bewusst sind und Wissenstransfer betreiben, um Zu-

[296] Die in dieser Tabelle dargestellten Zusammenhänge sind für Unternehmen mit zunehmender Mitarbeiterzahl von Relevanz, da mit diesem Anstieg sowohl die Implementierung von RM- als auch WM-Initiativen zunimmt (siehe hierzu auch die Korrelationen in Tab. 34 auf Seite 286).

gang zu externem Wissen zur erlangen. Auf der anderen hat die gleichzeitige Implementierung von RM-Initiativen zur Folge, dass diese Unternehmen eine vergleichsweise höhere Sensibilität für Risiken haben. Beide Faktoren zusammen dürften zum Erfolg des Wissenstransfers positiv beitragen. Die Mittelwertvergleiche zu den anderen Teilstichproben weisen keine signifikanten Unterschiede auf.
Insgesamt schätzen Großunternehmen im Vergleich zu mittelständischen Unternehmen den Wissenstransfer erfolgreicher ein, wobei diese Einschätzungen in Bezug auf die beiden Variablen Qualität und Quantität externen Wissens signifikant sind. Hinsichtlich Branchenzugehörigkeit bestehen keinerlei signifikante Abweichungen. Zudem schätzen Unternehmen, die sowohl WM- als auch RM-Initiativen implementiert haben, im Vergleich zu Unternehmen ohne Maßnahmen in diesem beiden Bereichen Wissensrisiken im Kontext des Wissenstransfers in Bezug auf alle fünf Variablen geringer ein.

7.2.5 Wissensqualität

Im nachfolgenden Abschnitt werden die sechs Variablen, die zur Messung des Konzeptes Wissensqualität herangezogen wurden, deskriptiv betrachtet.

n=129				**Wert der Likert Skala**						
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Korrektheit	5,02	5	1,20	7	47	36	26	7	6	0
Verfügbarkeit	5,02	5	1,49	19	41	27	18	16	6	2
Nachvollziehbarkeit	4,91	5	1,51	15	40	32	17	13	10	2
Aktualität	4,85	5	1,23	10	29	44	31	8	7	0
Rechtzeitigkeit	4,67	5	1,45	11	30	38	17	22	10	1
Anwendbarkeit	4,60	5	1,21	5	26	39	38	13	8	0

Tab. 48 Verteilung und Lageparameter zum Konzept Wissensqualität

In Tab. 48 sind die Lageparameter, die Standardabweichung und die Verteilung der Zustimmung zu den Aussagen abgetragen, wobei der absteigende Mittelwert das 1. Ordnungskriterium und aufgrund des gleichen Mittelwertes die aufsteigende Standardabweichung das 2. Ordnungskriterium darstellen. Insgesamt weist das Konzept Wissensqualität im Vergleich zu den anderen Konzepten die höchsten Mittelwerte auf. Die Variablen Korrektheit und Verfügbarkeit weisen jeweils einen Mittelwert von 5,02 auf, während die Anwendbarkeit von Wissen mit 4,6 durch den geringsten Mittelwert charakterisiert ist.

		Mitarbeiterzahl				
		a	b	c	d	
	n=129	n=12	n=12	n=83	n=22	**Δ**
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
Korrektheit	5,02	5,00	5,00	4,86	5,68	0,83*
Nachvollziehbarkeit	4,91	5,00	4,42	4,84	5,41	0,57
Aktualität	4,85	5,08	5,08	4,72	5,09	0,37
Rechtzeitigkeit	4,67	4,50	4,75	4,63	4,86	0,24
Anwendbarkeit	4,60	5,00	4,33	4,63	4,41	-0,22
Verfügbarkeit	5,02	5,08	5,25	5,02	4,86	-0,16

Tab. 49 Wissensqualität im Kontext der Unternehmensgröße

Betrachtet man das Konzept Wissensqualität im Kontext der Unternehmensgröße so ergeben sich bezogen auf die verschiedenen Teilstichproben folgende Mittelwerte (siehe Tab. 49). Das primäre Ordnungskriterium der Tabelle

stellt dabei wiederum die absolute Mittelwertabweichung zwischen Groß- und mittleren Unternehmen dar. Ein Vergleich der Mittelwerte in beiden Teilstichproben zeigt, dass die Wissensqualität in Großunternehmen bei vier von sechs Variablen höher eingeschätzt wird, während im Falle der Variablen Verfügbarkeit und Anwendbarkeit mittlere Unternehmen höhere Mittelwerte aufweisen. Bei der Überprüfung der Signifikanz dieser Abweichungen durch T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}0167$[297], ist allerdings nur die Abweichung in Bezug auf die Variable Korrektheit signifikant.

n=129	**Branchenzugehörigkeit**			a	b	
				n=50	n=79	**Δ**
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
Verfügbarkeit	4,50	5,02	5,75	4,72	5,22	-0,50
Nachvollziehbarkeit	4,41	4,91	6,00	4,66	5,08	-0,42
Aktualität	3,50	4,85	6,00	4,68	4,96	-0,28
Rechtzeitigkeit	3,80	4,67	5,50	4,50	4,77	-0,27
Anwendbarkeit	4,00	4,60	5,20	4,48	4,67	-0,19
Korrektheit	3,75	5,02	5,60	5,04	5,01	0,03

Tab. 50 Wissensqualität im Kontext der Branchenzugehörigkeit

Neben Unterschieden, die auf variierende Mitarbeiterzahl der Unternehmen zurückgeführt werden können, nimmt auch die Branchenzugehörigkeit Einfluss auf dieses Konzept. In Tab. 50 werden zu diesem Zweck die Mittelwerte der Teilstichproben produzierender und dienstleistungsorientierter Unternehmen miteinander verglichen und ausgehend von ersteren die Höhe der Differenz als Ordnungskriterium herangezogen. Fünf der sechs Variablen werden durch dienstleistungsorientierte Unternehmen höher bewertet, wobei keine dieser Abweichungen zwischen den Teilstichproben bei Zugrundelegung von T-Tests und einem analogen bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}0167$ signifikant ist. Neben der Größenklasse und der Branchenzugehörigkeit wird nachfolgend der Einfluss von WM- und RM-Initiativen auf die Einschätzung der Wissensqualität analysiert.

		RM und WM						
		a	**b**	**c**	**d**			
	n=129	n=50	n=11	n=28	n=40	**Δ**	**Δ**	**Δ**
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
Nachvollziehbarkeit	4,91	4,28	5,45	4,96	5,53	0,57	0,08	1,25*
Rechtzeitigkeit	4,67	4,10	4,64	4,93	5,20	0,27	0,56	1,1*
Verfügbarkeit	5,02	4,56	5,27	4,96	5,58	0,62	0,31	1,02*
Korrektheit	5,02	4,52	5,09	5,21	5,50	0,29	0,41	0,98*
Aktualität	4,85	4,32	5,00	5,14	5,28	0,14	0,28	0,96*
Anwendbarkeit	4,60	4,40	5,09	4,50	4,78	0,28	-0,31	0,38

Tab. 51 Wissensqualität im Kontext RM- und WM-Initiativen

Im Hinblick auf die verschiedenen Teilstichproben werden primär Unternehmen betrachtet, die Initiativen in beiden Bereichen implementiert haben, und als Ordnungskriterium Mittelwertabweichungen

[297] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/6=0{,}0167$.

zu Unternehmen ohne Maßnahmen herangezogen. Die Abweichungen in Tab. 51 machen deutlich, dass die Wissensqualität in Unternehmen, die RM- und WM-Initiativen einsetzen, vergleichsweise höher eingeschätzt wird. Legt man den T-Tests ein adjustiertes Signifikanzniveau von $\alpha^*=0{,}0167$ zugrunde, so sind die Unterschiede in fünf Fällen signifikant. Lediglich die Variable Anwendbarkeit von Wissen ist nicht signifikant. Betrachtet man ausgehend von Unternehmen mit Maßnahmen in beiden Bereichen Mittelwertabweichungen zu Unternehmen mit Initiativen nur in einem der beiden Bereiche, so ergeben sich keine signifikanten Unterschiede[298]. Die Abweichungen können einerseits auf das erhöhte Bewusstsein für den Wert von Wissen, das sich WM-Initiativen ergibt, und andererseits auf Verpflichtungen zum RM bzw. korrespondierende Initiativen zurückgeführt werden.
Insgesamt werden die Variablen des Konzeptes Wissensqualität in der Relation zu den anderen Konzepten am höchsten bewertet. Großunternehmen schätzen die Wissensqualität in Bezug auf die Korrektheit signifikant höher ein, während die Branchenzugehörigkeit keinen Einfluss auf die Einschätzung der Variablen nimmt. Hinsichtlich implementierter RM- und WM-Maßnahmen schätzen Unternehmen mit Maßnahmen in beiden Bereichen im Vergleich zu Unternehmen ohne Maßnahmen fünf der sechs Variablen signifikant höher ein.

7.2.6 Zusatzfragen

Neben den Fragen zu den fünf Konzepten wurde eine weitere Frage zur Bedeutung der Ressource Wissen für die Wertschöpfung und die Erstellung der Wertschöpfung und die Begründung von Wettbewerbsvorteilen in den Interviewleitfaden integriert und ebenfalls gemäß der Likert Skala kodiert. Analog zu den Auswertungen der Konzepte erfolgt mithilfe von Tab. 52 eine integrierte Betrachtung dieser Variable. Generell wird die Bedeutung der Ressource Wissen sehr hoch eingeschätzt, was sich in einem Mittelwert von 6,01 und einem Median von 6 niederschlägt. Dabei haben in 82,17% der Fälle die Interviewpartner der entsprechen Aussage zugestimmt oder stark zugestimmt. Im Hinblick auf die Unternehmensgröße wird in den befragten Großunternehmen die Bedeutung der Ressource Wissen mit einem Mittelwert von 6,23 am höchsten bewertet, gefolgt von kleinen und mittleren Unternehmen mit einem Mittelwert von 6,17 bzw. 6,01. In Kleinstunternehmen wird die Bedeutung mit 5,42 am geringsten bewertet. Diese Unterschiede weisen jedoch keine statistische Signifikanz auf. Betrachtet man die Branchen zusammengefasst als produzierende und dienstleistungsorientierte Unternehmen weichen die Mittelwerte mit 6,04 bzw. 5,99 gering voneinander ab und unterscheiden sich dabei nicht signifikant voneinander. Im Hinblick auf die Betrachtung der verschiedenen Teilstichproben in Bezug auf implementierte RM- und WM-Initiativen, weichen die Mittelwerte bei Unternehmen, die Maßnahmen in beiden Bereichen implementiert haben, von denen, die keine Initiativen betreiben um 0,67

[298] Die in dieser Tabelle dargestellten Zusammenhänge sind für Unternehmen mit zunehmender Mitarbeiterzahl von Relevanz, da mit diesem Anstieg sowohl die Implementierung von RM- als auch WM-Initiativen zunimmt (siehe hierzu auch die Korrelationen in Tab. 34 auf Seite 286).

n=129			Wert der Likert Skala						
x	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
6,01	6	1,26	53	53	8	6	5	3	1
			Mitarbeiterzahl						
					a	b	c	d	
					n=12	n=12	n=83	n=22	**Δ**
					-9	**-49**	**-249**	**>250**	**d-c**
					5,42	6,17	6,01	6,23	0,22
			Branchenzugehörigkeit						
							a	b	
							n=50	n=79	**Δ**
					Min	**Max**	**C-F**	**G-O**	**a-b**
					4,2	6,6	6,04	5,99	0,05
			RM und WM						
			a	b	c	d			
			n=50	n=11	n=28	n=40	**Δ**	**Δ**	**Δ**
			WM (-) RM (-)	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
			5,58	6,73	6,14	6,25	0,11	-0,48*	0,67*

Tab. 52 Bedeutung der Ressource in Bezug auf verschiedene Kriterien

ab, wobei die Abweichung unter Zugrundelegung eines Signifikanzniveau von $\alpha \leq 0{,}05$ dieser Einzeltest signifikant ist. Bei analogem Signifikanzniveau sind auch die Abweichungen zwischen Unternehmen mit Maßnahmen in beiden Bereichen und Unternehmen, die nur WM-Initiativen implementiert haben, signifikant. Unternehmen, die nur WM-Initiativen einsetzen, schätzen die Bedeutung der Ressource Wissen mit einem Mittelwert von 6,73 vergleichen mit den Unternehmen der anderen Teilstichproben am höchsten ein.

Neben der Bedeutung der Ressource Wissen wurde auch die Höhe der externen Mitarbeiterfluktuation erhoben und untersucht, wie sich eine entsprechende Fluktuationsrate auf die Wissensrisikowahrnehmung auswirkt. Ausgehend von 126 Unternehmen, die entsprechende Angaben gemacht haben, liegt die externe Fluktuation bei 80,95% der Unternehmen im Bereich von bis zu 5%. Fluktuationswerte über 20% wurden nicht angegeben (siehe Tab. 53).

n=126[299]			Wert der Likert Skala						
			>25%	**20-24%**	**15-19%**	**10-14%**	**6-9%**	**2-5%**	**≤1%**
Variable		**x**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
externe Mitarbeiter-fluktuation	gesamt	1,97	0	0	3	12	9	56	46
	1-9 MA	1,58	0	0	0	1	1	2	8
	10-49 MA	1,92	0	0	1	1	0	4	6
	50-249 MA	2,04	0	0	2	9	7	35	28
	>250 MA	1,95	0	0	0	1	1	15	4
	C-F	1,88	0	0	1	3	3	18	23
	G-O	2,09	0	0	2	9	6	36	23

Tab. 53 Verteilung der externen Mitarbeiterfluktuation

[299] In drei Fällen wurde keine Angabe zur Fluktuation gemacht.

Bei Kleinstunternehmen liegt der Fokus bei 66,67% der betrachten Unternehmen bei einer Fluktuation kleiner oder gleich 1%. Dies trifft auch auf kleine Unternehmen zu, von denen 50% ebenfalls eine externe Fluktuation in diesem Bereich aufweist. Bei mittleren und großen Unternehmen ergibt sich ein anderes Bild. So liegt bei mittleren Unternehmen mit 43,21% der Schwerpunkt im Intervall 2-5%, während dies auch auf 71,43% der Großunternehmen zutrifft. Dabei sind weder die Mittelwertdifferenzen zwischen Großunternehmen und mittelständischen Unternehmen[300] noch die Abweichungen zwischen produzierenden und dienstleistungsorientierten Unternehmen[301] bei einem Signifikanzniveau von $\alpha \leq 0{,}05$ signifikant. Neben den Unterschieden der Fluktuation bezogen auf die Schichtungsmerkmale Unternehmensgröße und Branchenzugehörigkeit wurden die Unternehmen in Abhängigkeit der Höhe der Fluktuation in drei Teilstichproben aufgeteilt. Zum einen wurden 15 Unternehmen zu einer Gruppe zusammengefasst, die eine Fluktuation von 10% oder mehr aufweisen. Als zweite Gruppe wurden 65 Unternehmen zusammengefasst, deren Fluktuation im Intervall von 2-9% liegt. Die dritte Gruppe bilden 46 Unternehmen, die durch eine Fluktuation von 1% oder weniger charakterisiert sind. Für diese drei Gruppen werden die Variablen Vertretung, Nachbesetzung, nachteilige Mitarbeiterfluktuation, Konkurrenzschutzklauseln und Geheimhaltungsvereinbarungen gesondert betrachtet, da sie mit der Fluktuation in Zusammenhang stehen. So könnte bei den beiden erstgenannten Variablen vermutet werden, dass in Unternehmen mit höherer Fluktuation Vertretungs- und Nachbesetzungsprobleme relevanter sind. Ebenso könnte das Risiko einer nachteiligen Mitarbeiterfluktuation in Unternehmen mit höherer Fluktuation auch höher eingeschätzt werden. Die beiden letztgenannten Steuerungsmaßnahmen könnten möglicherweise eine Reaktion auf höhere Fluktuationsquoten darstellen. In Tab. 54 werden die Unterschiede im Hinblick auf die Mittelwerte zwischen den Gruppen dargestellt, wobei ausgehend von Unternehmen mit einer geringen Fluktuationsquote die Mittelwertabweichungen abgetragen sind.

Mitarbeiterfluktuation	**a**	**b**	**c**		
	n=46	**n=65**	**n=15**		
	≤ 1%	**2-9%**	**≥10%**	**Δ**	**Δ**
Variable	**x**	**x**	**x**	**a-b**	**a-c**
Vertretung	3,74	3,68	4,67	0,06	-0,93
Nachbesetzung	3,61	3,63	4,47	-0,02	-0,86
nachteilige Mitarbeiterfluktuation	3,24	3,32	3,93	-0,08	-0,69
Konkurrenzschutzklauseln	3,67	3,6	3,07	0,07	0,6
Geheimhaltungsvereinbarungen	4,54	5,05	4,47	-0,51	0,07

Tab. 54 Zusammenhänge der externen Mitarbeiterfluktuation

Als Ordnungskriterium für Tab. 54 wird die absolute Mittelwertabweichung zwischen Unternehmen mit einer Fluktuation von 1% oder weniger und Unternehmen mit einer externen Fluktuationsquote von 10% oder mehr herangezogen. Während Vertretungs-, Nachbesetzungsprobleme und die nachteilige Mitarbeiterfluktuation in den Teilstichproben a und b nur gering abweichen, weisen Unternehmen mit einer Fluktuation von 10% und mehr höhere Mittelwerte auf, wobei die Abweichungen bei einem

[300] Die Mittelwertabweichung zwischen den Teilstichproben beträgt 0,12.
[301] Die Mittelwertabweichung zwischen den Teilstichproben beträgt 0,21.

adjustierten Signifikanzniveau von $\alpha^*=0{,}02$[302] nicht signifikant sind. Somit nimmt eine höhere Fluktuation keinen signifikanten Einfluss auf die relevanten Variablen.

7.2.7 Diskussion

Betrachtet man die in den vorangegangenen Abschnitten dargestellten Ergebnisse im Zusammenhang, so lassen sich folgende zentrale Ergebnisse der Studie zusammenfassen. Vergleicht man die Mittelwerte über die fünf Konzepte hinweg, so werden die vier Variablen Korrektheit (5,02), Verfügbarkeit (5,02), Nachvollziehbarkeit (4,91) und Aktualität (4,85), die dem Konzept Wissensqualität zugeordnet sind, am höchsten eingeschätzt. Darauf folgen die beiden Variablen IT-Sicherheitsrichtlinien (4,81) und IT-Sicherheitsbewusstsein (4,79), die Bestandteil des Konzeptes Steuerung von Wissensrisiken sind. Am niedrigsten werden die beiden Variablen unautorisierte Zugriffe (2,15) und Competitive Intelligence (2,39) bewertet, die zur Messung des Konzeptes Wissensdiffusion dienen und zugleich korrespondierende Risiken darstellen. Die Variable Verlust dokumentierten Wissens (2,47), die dem Konzept Wissensverlust zugeordnet ist, wird am drittniedrigsten eingeschätzt.

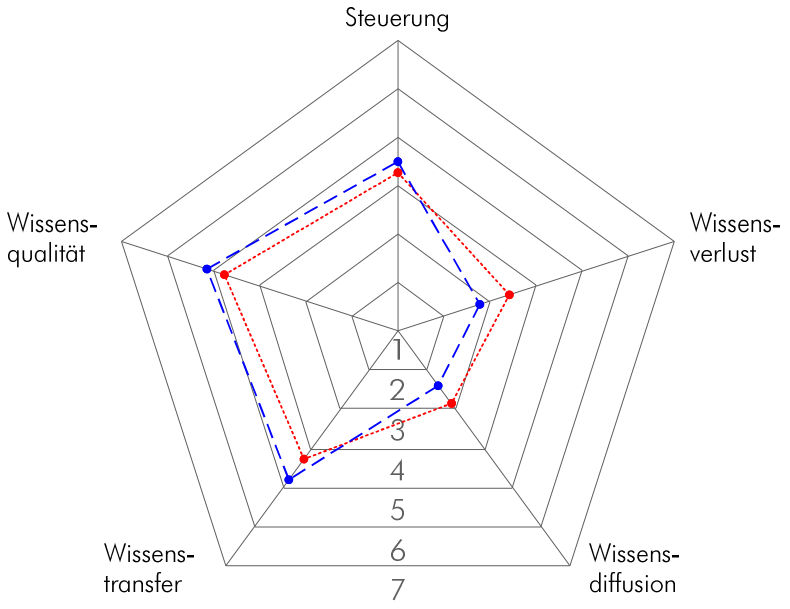
		Mitarbeiterzahl				
		a	b	c	d	
	n=129	n=12	n=12	n=83	n=22	**Δ**
Variable	**x**	**≤9**	**≤49**	**≤249**	**>250**	**d-c**
Wissensverlust						
Nichtdokumentation (TG)	3,86	4,58	4,17	3,94	3,00	-0,94*
Nichtdokumentation (PG)	3,47	4,17	3,92	3,49	2,73	-0,77*
Wissenstransfer						
Qualität externen Wissens	4,69	4,50	4,92	4,53	5,27	0,74*
Quantität externen Wissens	4,25	3,75	4,50	4,12	4,86	0,74*
Wissensqualität						
Korrektheit	5,02	5,00	5,00	4,86	5,68	0,83*

Tab. 55 signifikante Abweichungen im Kontext der Unternehmensgröße

Dabei ist zu beachten, dass insbesondere die Variablen, die dem Konzept Steuerung zugeordnet sind, eine vergleichsweise hohe Standardabweichung aufweisen und dadurch die Interpretation dieser Mittelwerte vorsichtig erfolgen muss. Die Variablen, die zur Messung des Konzeptes Wissensqualität herangezogen werden, streuen vergleichsweise weniger um den Mittelwert. Fasst man die Ergebnisse hinsichtlich der an der Mitarbeiterzahl gemessenen Unternehmensgröße zusammen (siehe Tab. 55), so ergeben sich folgende signifikanten Unterschiede, wobei in Bezug auf die beiden Konzepte Steuerung von Wissensrisiken und Wissensdiffusion keine der Variablen beim jeweilig adjustierten Signifikanzniveau signifikant ist. Im Hinblick auf das Konzept Wissensverlust schätzen Großunternehmen die Risiken der Nichtdokumentation von Wissen im Projekt- und im Tagesgeschäft signifikant geringer ein als mittelständische Unternehmen.

[302] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/5=0{,}02$.

Eine mögliche Begründung dafür ist darin zu sehen, dass Ansätze zur Dokumentation von Wissen in Großunternehmen verbreiteter sind. In Bezug auf das Konzept Wissenstransfer werden die Quantität und die Qualität externen Wissens in Großunternehmen signifikant höher eingeschätzt. Die Qualität des dokumentierten Wissens wird in Bezug auf die Variable Korrektheit von Wissen seitens Großunternehmen signifikant höher eingeschätzt (siehe Tab. 55).



	Groß-unternehmen	mittlere Unternehmen
Steuerung	4,68	4,20
Wissensverlust*	2,86	3,45
Wissensdiffusion*	2,48	2,99
Wissenstransfer	4,78	4,31
Wissensqualität	5,05	4,78

Abb. 35 Unterschiede zwischen Groß- und mittleren Unternehmen

Eine Erklärung könnte darin liegen, dass aufgrund der höheren Mitarbeiterzahl zusätzlich Rollen geschaffen werden können, die sich dediziert mit der Qualität des Wissens beschäftigen, wie dies beispielsweise bei Themenverantwortlichen der Fall ist, die in zahlreichen Großunternehmen eingesetzt werden. Bildet man die Mittelwerte über alle Variablen eines Konzeptes, so ergeben sich in Bezug auf die beiden Teilstichproben, die in Abb. 35 dargestellten Ausprägungen. So ist in Groß- im Vergleich zu mittelständischen Unternehmen die Steuerung von Wissensrisiken ausgeprägter, während Risiken in Bezug auf Wissensverluste und die Wissensdiffusion geringer eingeschätzt und auch der Wissenstransfer und die Wissensqualität positiver bewertet werden. Legt man das adjustierte Signifikanzniveau $\alpha^*=0{,}02$[303] zugrunde, so schätzen bei dieser aggregierten Betrachtung Großunternehmen die Wissensrisiken im Zusammenhang mit Wissensverlusten und Wissensdiffusionen signifikant geringer ein, während die Abweichungen bzgl. der anderen Konzepte nicht signifikant sind.

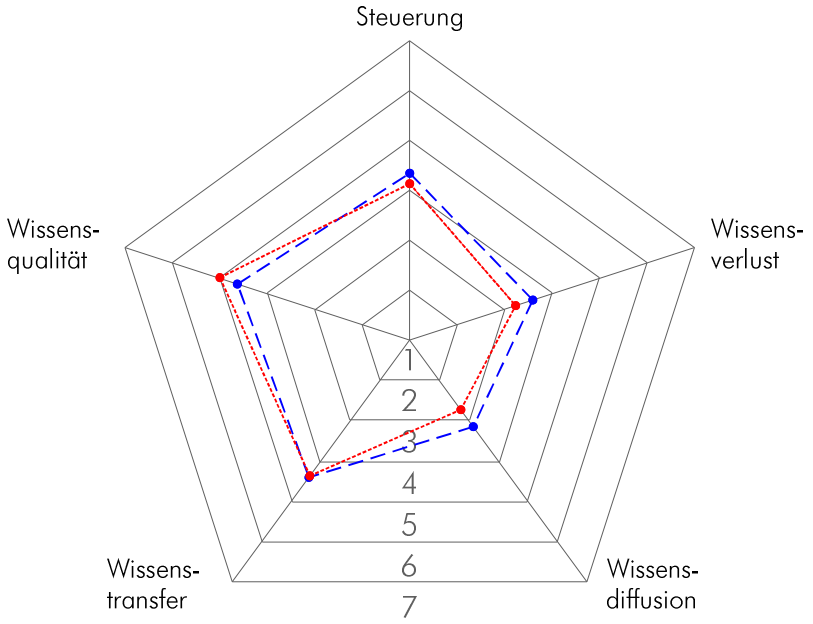
n=129	**Branchenzugehörigkeit**			a	b	
				n=50	n=79	**Δ**
Variable	**Min**	**x**	**Max**	**C-F**	**G-O**	**a-b**
Steuerung von Wissensrisiken						
gewerbliche Schutzrechte (IP)	2,00	3,65	4,53	4,28	3,25	1,03*

Tab. 56 signifikante Abweichungen im Kontext der Branchenzugehörigkeit

[303] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/5=0{,}02$.

Betrachtet man im Hinblick auf die Branchenzugehörigkeit als Teilstichproben produzierende und dienstleistungsorientierte Unternehmen, so ergibt unter Zugrundelegung der jeweils adjustierten Signifikanzniveaus über alle Variablen der fünf Konzepte eine signifikante Abweichung (siehe Tab. 56). So werden gewerbliche Schutzrechte in produzierenden Unternehmen signifikant umfassender eingesetzt. Diese Abweichung kann primär dadurch erklärt werden, dass bedingt durch den Charakter der Produkte gewerbliche Schutzrechte wie Patente vorwiegend in produzierenden Unternehmen zum Einsatz kommen.

Betrachtet man die fünf Konzepte über die beiden Teilstichproben aggregiert, so ergeben sich die in Abb. 36 dargestellten Zusammenhänge. So weisen produzierende Unternehmen eine stärkere Steuerung als dienstleistungsorientierte Unternehmen auf. Andererseits werden auch Risiken in Bezug auf den Verlust und die unerwünschte Diffusion von Wissen höher eingeschätzt und zudem die Qualität dokumentierten Wissens geringer bewertet. Legt man das adjustierte Signifikanzniveau $\alpha^*=0{,}02$[304] zugrunde, so sind diese Abweichungen jedoch nicht signifikant



	produz. Unternehmen	dienstleist. Unternehmen
Steuerung	4,39	4,18
Wissensverlust	3,58	3,27
Wissensdiffusion	3,12	2,79
Wissenstransfer	4,40	4,39
Wissensqualität	4,68	4,95

Abb. 36 Unterschiede zwischen produzierenden und dienstleistungsorientierten Unternehmen

Betrachtet man die verschiedenen Teilstichproben in Bezug auf die Implementierung von RM- und WM-Initiativen, so ergeben sich folgende signifikante Unterschiede, wobei die Teilstichprobe an Unternehmen, die Maßnahmen in beiden Bereichen implementiert haben, den Hauptuntersuchungsgegenstand darstellt. Im Hinblick auf das Konzept Steuerung von Wissensrisiken zeigt sich, dass Unternehmen mit WM- und RM-Initiativen umfassender Steuerungsmaßnahmen einsetzen, wobei bei Zugrundelegung des adjustierten Signifi-

[304] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/5=0{,}02$.

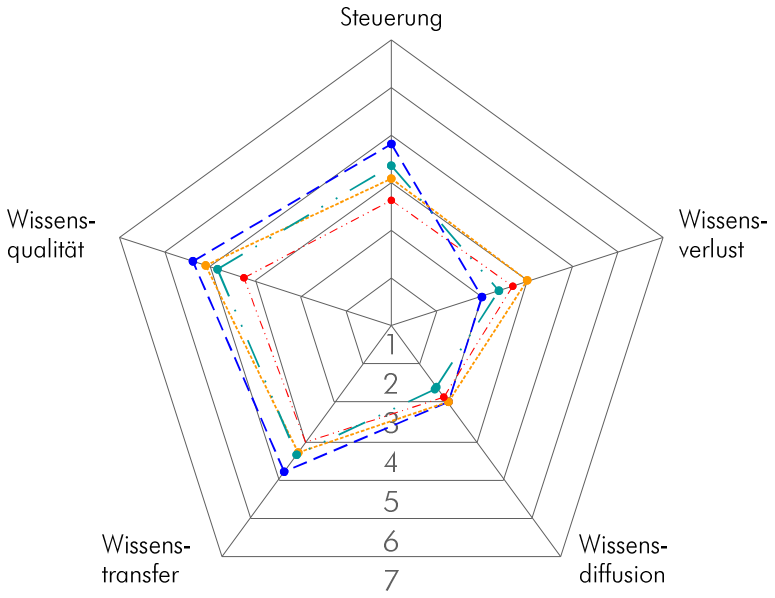
kanzniveaus neun Steuerungsmaßnahmen signifikant umfassender implementiert werden (siehe Tab. 57).

RM und WM								
		a	b	c	d			
	n=129	n=50	n=11	n=28	n=40	Δ	Δ	Δ
Variable	**x**	**WM (-) RM (-)**	**WM (+) RM (-)**	**WM (-) RM (+)**	**WM (+) RM (+)**	**d-c**	**d-b**	**d-a**
Steuerung von Wissensrisiken								
gewerbliche Schutzrechte (IP)	3,65	3,08	3,55	3,36	4,60	1,24	1,05	1,52*
Klassifikation von Wissen	4,50	3,90	4,09	4,46	5,40	0,94	1,31	1,50*
Wissenstransferrichtlinien	4,33	3,74	4,45	4,04	5,23	1,19	0,78	1,49*
IT-Sicherheitsrichtlinien	4,81	4,06	4,45	5,46	5,38	-0,08	0,93	1,32*
Dynamisierung der Zugriffsrechte	4,51	3,86	4,36	4,93	5,08	0,15	0,72	1,22*
Konkurrenzschutzklauseln	3,57	3,04	3,18	3,75	4,20	0,45	1,02	1,16*
Geheimhaltungsvereinbarungen	4,77	4,24	4,73	4,86	5,38	0,52	0,65	1,14*
Redundanzschaffung	3,90	3,40	3,82	3,93	4,53	0,6	0,71	1,13*
IT-Sicherheitsbewusstsein	4,79	4,18	4,91	5,32	5,15	-0,17	0,24	0,97*
Wissensverlust								
Nichtdokumentation (TG)	3,86	4,42	3,91	4,00	3,05	-0,95*	-0,86	-1,37*
Nichtdokumentation (PG)	3,47	3,90	3,73	3,43	2,88	-0,55*	-0,85	-1,02*
Verlust dokumentierten Wissens	2,47	2,78	3,18	2,29	2,00	-0,29	-1,18	-0,78*
Wissenstransfer								
Beitrag externen Wissens	4,73	4,26	4,45	4,68	5,43	0,75	0,98	1,17*
Erweiterung der Wissensbasis	4,33	3,86	4,18	4,29	5,00	0,71	0,82	1,14*
Quantität externen Wissens	4,25	3,92	4,18	4,18	4,73	0,55	0,55	0,81*
Qualität externen Wissens	4,69	4,48	4,27	4,54	5,18	0,64	0,91	0,7*
Reduktion der Abhängigkeit	3,95	3,64	4,36	3,96	4,23	0,27	-0,13	0,59*
Wissensqualität								
Nachvollziehbarkeit	4,91	4,28	5,45	4,96	5,53	0,57	0,08	1,25*
Rechtzeitigkeit	4,67	4,10	4,64	4,93	5,20	0,27	0,56	1,1*
Verfügbarkeit	5,02	4,56	5,27	4,96	5,58	0,62	0,31	1,02*
Korrektheit	5,02	4,52	5,09	5,21	5,50	0,29	0,41	0,98*
Aktualität	4,85	4,32	5,00	5,14	5,28	0,14	0,28	0,96*

Tab. 57 signifikante Abweichungen im Kontext von RM- und WM-Initiativen

Hinsichtlich des Konzeptes Wissensverlust werden in Unternehmen mit RM- und WM-Initiativen im Vergleich zu Unternehmen ohne derartige Initiativen die drei Wissensrisiken Nichtdokumentation im Tagesgeschäft, Nichtdokumentation im Projektgeschäft und Verlust dokumentierten Wissens signifikant geringer eingeschätzt. Die beiden Risiken zur Nichtdokumentation werden von Unternehmen, die nur RM-Maßnahmen implementiert haben, im Vergleich zu Unternehmen mit Maßnahmen in beiden Bereichen signifikant höher eingeschätzt (siehe Tab. 57). Die positiven Ausprägungen können zum einen auf eine stärkere Steuerung und zum anderen auf ein höheres Risikobewusstsein zurückgeführt werden. In Bezug auf Risiken im Bereich der Wissensdiffusion ergeben sich keine signifikanten Abweichungen zwischen den Teilstichproben. Im Hinblick auf das Konzept Wissenstransfer werden alle fünf zur Operationalisierung eingesetzten Variablen von Unternehmen, die RM- und WM-Initiativen implementiert haben, im Vergleich zu Unternehmen ohne Maßnahmen in diesen beiden Bereichen

signifikant höher eingeschätzt. Die Qualität dokumentierten Wissens wird in Unternehmen mit implementierten RM- und WM-Initiativen in Bezug auf alle sechs Variablen höher bewertet, wobei diese mit Ausnahme der Variable Anwendbarkeit von Wissen signifikant abweichen. Bei einer aggregierten Betrachtung der Mittelwerte bestätigen sich die zuvor betrachteten Signifikanzen (siehe Abb. 37).



		kein RM und WM (a)	nur WM (b)	nur RM (c)	RM und WM (d)
Steuerung	*(d-a)	3,78	4,11	4,35	4,83
Wissensverlust	*(d-b) / *(d-c)	3,62	4,03	3,53	3,00
Wissensdiffusion	/	2,87	3,00	2,76	3,05
Wissenstransfer	*(d-c)	4,03	4,29	4,33	4,91
Wissensqualität	*(d-a)	4,36	5,09	4,95	5,31

Abb. 37 Unterschiede im Hinblick auf RM- und WM-Initiativen

So weisen Unternehmen mit Maßnahmen in beiden Bereichen im Vergleich zu den anderen Teilstichproben die höchste Steuerung, die positivste Einschätzung der Wissensqualität und des Wissenstransfers sowie die niedrigste Einschätzung von Wissensverlusten auf. In Bezug auf die Wissensdiffusion nehmen diejenigen Unternehmen, die nur RM-Maßnahmen implementiert haben, die niedrigste Risikoeinschätzung vor. Signifikante Unterschiede bestehen bzgl. des Vergleichs von Unternehmen mit Maßnahmen in beiden Bereichen und denen ohne jegliche Maßnahmen bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}02$[305] in Bezug auf die Konzepte Steuerung und Wissensqualität, wobei erstere stärker implementiert ist und die Wissensqualität positiver eingeschätzt wird (siehe Abb. 37). Beim Vergleich der Teilstichproben an Unternehmen mit Maßnahmen in beiden Bereichen und denjenigen, die nur RM-Maßnahmen implementiert haben, werden von erstgenannter Teilstichprobe Wissensverluste signifikant geringer und der Wissenstransfer signifikant positiver eingeschätzt. Unternehmen, die nur WM-Initiativen implementiert haben, schätzen im Vergleich zu Unternehmen mit Maßnahmen in beiden Bereichen Wissensverluste signifikant höher ein (siehe Abb. 37). Dies kann so interpretiert werden, dass implementierte RM-Maßnahmen Wissensverluste bzw. die korrespondierende Einschätzung reduzieren. Insbesondere bei der Teilstichprobe der Unternehmen, die nur WM-Initiativen implementiert haben, sind die Ergebnisse aufgrund des geringen Stichprobenumfangs vorsichtig zu interpretie-

[305] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/5=0{,}02$.

ren. Nachdem eine deskriptive Analyse der einzelnen Konzepte und der entsprechenden Variablen vorgenommen wurde, besteht das Ziel des nachfolgenden Abschnittes darin Zusammenhänge zwischen den Variablen zu identifizieren.

7.3 Betrachtung ausgewählter Einflüsse der Steuerungsmaßnahmen

Nachdem die einzelnen Konzepte isoliert voneinander betrachtet und vorwiegend der Einfluss der Unternehmensgröße, Branchenzugehörigkeit sowie bestehender RM- und WM-Initiativen analysiert wurde, wir im folgenden Abschnitt der Einflusses der Steuerungsmaßnahmen auf die vier zentralen Konzepte analysiert.

Den Ausgangspunkt für eine derartige Betrachtung bildet dabei die Tatsache, dass eine umfassendere Implementierung einer Steuerungsmaßnahme zur Folge haben sollte, dass zu steuernde Risiken abnehmen, ohne allerdings zugleich Risikopotentiale in anderen Bereichen zu eröffnen. Dies muss aber nicht der Fall sein, da auch negative Effekte von Steuerungsmaßnahmen ausgehen können, die deren effizienten Einsatz behindern können. Aus diesem Grund stellt die Identifikation potentieller Austauschbeziehungen bzw. negativer Effekte, die es beim Ergreifen der Maßnahme zu beachten gilt, den Gegenstand dieses Abschnittes dar. Um eine derartige Analyse des Einflusses der Steuerungsmaßnahmen vornehmen zu können, werden Unternehmen in Abhängigkeit des Grades der Zustimmung zur Aussage, die auf die Implementierung der jeweiligen Steuerungsmaßnahme bezogen ist, in Teilstichproben eingeteilt. Diese Unterteilung legt die Prämisse zugrunde, dass die Steuerung vergleichsweise gering ist, wenn die entsprechende Aussage mit 1-4 beantwortet wurde und eine hohe Steuerung in einem Zustimmungsbereich von 5-7 vorliegt. Dabei wird diese Prämisse dadurch gestützt, dass der aggregierte Mittelwert über alle Steuerungsmaßnahmen 4,26 beträgt und somit eine stärkere bzw. überdurchschnittliche Steuerung mit den Ausprägungen über den Likert Wert 5 einhergeht. Die jeweilige Verteilung des Implementierungsgrades der Steuerungsmaßnahme wird bei der nachfolgenden Analyse der Teilstichproben sowohl in Tab. 58 als auch im nachfolgenden Text in eckigen Klammern angegeben, wobei die erste Ziffer die Anzahl der Unternehmen repräsentiert, die die entsprechend dieser Einteilung die Steuerungsmaßnahme in geringerem Umfang implementiert haben. Ausgehend von stärker steuernden Unternehmen sollte sich demnach ein umfassenderes Ergreifen einer Steuerungsmaßnahme auf eine geringere Einschätzung und somit einen geringeren Mittelwert in Bezug auf die Konzepte Wissensverlust und Wissensdiffusion auswirken. Hinsichtlich der positiv operationalisierten Konzepte Wissenstransfer und Wissensqualität sollten sich zugleich geringere Wissensrisikoausprägungen zugunsten stärker steuernder Unternehmen einstellen. Stärker ausgeprägte Wissensrisiken sind durch Unterstreichung in Tab. 58 kenntlich gemacht.

Steuerungsmaßnahme / Wissensrisiko		Klassifikation von Wissen	Zutrittsbeschränkung	Zugriffsbeschränkung	Dynamisierung Zugriffsrechte	Geheimhaltungsvereinbarungen	Wissenstransferrichtlinien	Begrenzung der Interaktion	Kooperationsvereinbarungen	Konkurrenzschutzklauseln	IT-Sicherheitsrichtlinien	IT-Sicherheitsbewusstsein	gewerbliche Schutzrechte	Redundanzschaffung	**Σ Einfluss (max. 13)**
Teilstichproben [1-4/5-7]		[59/70]	[62/67]	[65/64]	[59/70]	[53/76]	[64/65]	[59/70]	[90/39]	[82/47]	[52/77]	[46/83]	[82/47]	[76/53]	- / +
Wissensverlust (-)	Nichtdokumentation (Tagesgeschäft)	-0,76	-0,55	-0,13	-0,51	-0,78	-0,93	-0,66	-0,65	-0,95	-0,56	-1,13	-0,68	-0,53	0 / 4
	Nichtdokumentation (Projektgeschäft)	-0,77	0,41	-0,58	-0,95	-1,20	-1,00	-0,74	-0,52	-0,80	-0,67	-0,73	-0,26	-0,85	0 / 6
	Nachbesetzung	0,00	0,32	0,26	0,22	-0,20	-0,07	0,06	0,13	0,26	-0,23	-0,08	0,19	-0,15	0 / 0
	Vertretung	-0,34	0,26	-0,10	-0,09	-0,44	-0,31	-0,09	0,23	-0,04	-0,41	-0,59	0,09	-0,48	0 / 0
	Reorganisation	-0,30	0,20	0,20	0,36	-0,56	-0,17	0,11	0,17	-0,11	-0,02	-0,49	-0,18	-0,46	0 / 0
	Verlust dokumentierten Wissens	-0,83	-0,38	0,04	-0,36	-0,62	-0,57	-0,20	-0,52	-0,70	-0,70	-0,76	-0,33	-0,66	0 / 2
Wissensdiffusion (-)	unautorisierte Zugriffe	0,08	0,00	-0,20	0,21	-0,20	0,23	0,02	0,56	0,34	0,02	0,03	0,50	0,17	0 / 0
	nachteilige Mitarbeiterfluktuation	0,67	0,39	0,05	0,61	0,39	0,54	0,20	0,56	-0,20	0,09	0,12	0,21	0,12	0 / 0
	Reverse Engineering	0,09	0,38	0,56	0,18	-0,46	-0,18	-0,26	0,75	-0,32	-0,07	0,46	0,05	0,36	0 / 0
	Imitation	0,10	0,33	0,13	0,44	-0,37	0,06	-0,24	0,39	-0,19	0,10	0,22	0,12	-0,24	0 / 0
	Competitive Intelligence	-0,19	0,40	0,32	0,37	-0,50	-0,04	-0,04	0,55	-0,14	0,00	0,03	-0,01	-0,11	0 / 0
	unerwünschter Zugang für Partner	-0,19	(0,08)	0,29	0,25	-0,24	0,15	0,37	0,24	0,30	0,25	0,11	0,34	0,47	0 / 0
Σ Einfluss Wissensverlust und -diffusion (max. 12)		3 / 0	0 / 0	0 / 0	1 / 0	1 / 0	2 / 0	0 / 0	0 / 0	3 / 0	0 / 0	1 / 0	0 / 0	1 / 0	
Wissenstransfer (+)	Erweiterung der Wissensbasis	0,52	0,58	0,52	0,96	0,82	0,69	0,80	0,44	0,68	0,69	0,59	0,31	0,94	0 / 4
	Beitrag externen Wissens	0,84	0,78	0,45	0,81	0,76	0,86	0,97	0,61	0,93	0,54	0,86	0,16	0,75	0 / 9
	Reduktion der Abhängigkeit	0,26	0,16	0,74	0,54	0,18	0,71	0,48	0,80	0,78	0,86	0,60	0,24	0,88	0 / 4
	Qualität externen Wissens	0,40	0,71	0,58	0,62	0,43	0,38	0,65	0,11	0,35	0,32	0,63	0,02	0,33	0 / 3
	Quantität externen Wissens	0,36	0,66	0,53	0,89	0,49	0,43	0,64	0,27	0,25	0,16	0,59	0,25	0,41	0 / 1
Wissensqualität (+)	Verfügbarkeit	0,79	0,11	0,29	0,57	0,23	0,95	0,76	0,26	0,57	0,33	0,85	-0,14	0,60	0 / 4
	Nachvollziehbarkeit	0,84	0,46	0,11	0,69	0,53	1,13	0,62	0,45	0,44	0,44	0,75	0,03	0,72	0 / 3
	Rechtzeitigkeit	1,17	0,41	0,66	0,51	0,65	0,95	0,92	0,55	0,62	0,41	0,93	0,12	1,01	0 / 5
	Korrektheit	0,79	0,39	0,39	0,85	0,49	0,76	0,45	0,19	0,57	0,52	0,95	0,70	0,83	0 / 6
	Aktualität	0,73	0,49	0,45	0,79	0,61	0,86	0,42	0,51	0,47	0,37	0,55	0,27	0,67	0 / 4
	Anwendbarkeit	0,54	-0,09	-0,01	0,32	0,34	0,72	0,26	0,43	0,20	0,16	0,35	-0,10	0,59	0 / 2
Σ Einfluss gesamt (max. 23)		9 / 0	2 / 0	1 / 0	7 / 0	3 / 0	10 / 0	5 / 0	0 / 0	4 / 0	1 / 0	5 / 0	1 / 0	9 / 0	57 / 0

Tab. 58 Mittelwertabweichungen im Kontext der Steuerungsintensität

Insbesondere diese potentiellen Effekte sind beim Einsatz der Steuerungsmaßnahme zu beachten. In Tab. 58 sind die Signifikanzen abgetragen und grau hinterlegt. Diese wurden für jede einzelne Steuerungsmaßnahme durch die Analyse der Mittelwertabweichungen mittels T-Tests zu einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}004$[306] ermittelt. Signifikante Abweichungen sind in den jeweiligen Randsummen von Tab. 58 abgetragen, wobei geringere Wissensrisikoausprägungen das jeweils obere und höhere Wissensrisikoausprägungen das untere Feld der Randsumme einnehmen. Diese zusammenfassende Betrachtung zeigt, dass zwar höhere Wissensrisikoausprägungen bestehen, aber keine dieser Abweichungen signifikant ist. Somit stehen die 13 Steuerungsmaßnahmen nur mit signifikant geringeren Wissensrisikoausprägungen in Zusammenhang, wobei in der Spitze 10 der 23 Variablen signifikant positiv abweichen.

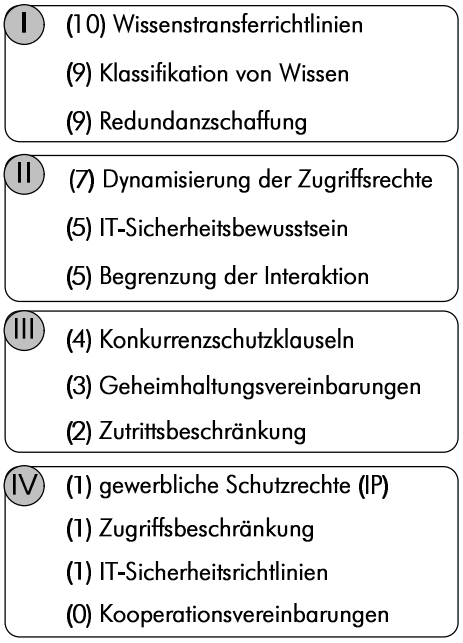


Abb. 38 Gruppierung der Steuerungsmaßnahmen nach signifikanten Zusammenhängen

Im Folgenden werden die Steuerungsmaßnahmen entsprechend der Anzahl an signifikanten Abweichungen gruppiert, während bei der Diskussion der einzelnen Steuerungsmaßnahmen erörtert wird, inwiefern diese Abweichungen sachlogisch einer umfassenderen Implementierung der Steuerungsmaßnahmen zugerechnet werden können.

So werden in Kategorie I Steuerungsmaßnahmen mit 8 oder mehr geringeren Wissensrisikoausprägungen, in Kategorie II Steuerungsmaßnahmen mit zwischen fünf bis sieben geringeren Wissensrisikoausprägungen und in Kategorie III Steuerungsmaßnahmen, die mit zwischen zwei und vier geringeren Wissensrisikoausprägungen in Zusammenhang stehen, eingeordnet. Kategorie IV umfasst schließlich Steuerungsmaßnahmen mit einer oder keiner geringeren Wissensrisikoausprägung. Nachfolgend wird auf der Ebene dieser Kategorien erörtert, inwiefern die geringeren Wissensrisikoausprägungen mit der umfassenden Steuerung erklärt werden können. Die Diskussion innerhalb der Kategorie erfolgt absteigend nach der Anzahl der geringeren Wissensrisikoausprägungen.

Kategorie I: Die umfassendere Implementierung der Steuerungsmaßnahmen Wissenstransferrichtlinien, Klassifikation von Wissen und Redundanzschaffung steht im Hinblick auf die 23 Wissensrisiken in Zusammenhang mit acht bis zehn geringeren Wissensrisikoausprägungen. Die Zusammenhänge werden im Folgenden sachlogisch interpretiert.

[306] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/23 = 0{,}004$.

- **Wissenstransferrichtlinien**: [64/65] Auf Basis theoretischer Vorüberlegungen wurde bei Wissenstransferrichtlinien ein Einfluss auf die Konzepte Wissenstransfer und Wissensdiffusion vermutet und dieser Einfluss als indifferent eingeschätzt, da insbesondere eine Hemmung des Wissenstransfers denkbar ist. Im Hinblick auf den durchgängig positiv bewerteten Wissenstransfer sind die Abweichungen zwischen den Teilstichproben in Bezug auf die Variablen Erweiterung der Wissensbasis, Beitrag zu anderen Aufgaben und Reduktion von Abhängigkeiten signifikant. Hinsichtlich dieser Steuerungsmaßnahme kann interpretiert werden, dass klare Regelungen insbesondere den erwünschten Wissenstransfer positiv beeinflussen. So kann umgekehrt bei Unternehmen, die geringer steuern, der geringer eingeschätzte Wissenstransfererfolg darauf zurückgeführt werden, dass Unsicherheiten über die Transferierbarkeit des Wissens bestehen und somit Wissen von den Mitarbeitern zurückgehalten wird.
- **Klassifikation von Wissen**: [59/70] Bei der Konzeption der Studie wurde davon ausgegangen, dass die Steuerungsmaßnahmen Klassifikation von Wissen auf alle vier Konzept Einfluss hat, da durch deren Implementierung Anhaltspunkte bestehen, wie werthaltig bzw. schützenswert vorhandenes Wissen ist. Geht man von der Teilstichprobe von Unternehmen mit einer höheren Steuerung aus, so ergeben sich signifikant geringere Wissensrisikoausprägungen bei fünf der sechs Variablen zur Operationalisierung der Wissensqualität (siehe Tab. 58). Die höhere Ausprägung in Bezug auf die Wissensqualität können dahingehend interpretiert werden, dass Unternehmen, die Wissen umfassender klassifizieren, durch ein vergleichsweise höheres Bewusstsein für den Wert des Wissens charakterisiert sind und somit stärker auf Qualität von Wissen fokussieren. Auf der anderen Seite sind Unternehmen, die Wissen stärker klassifizieren, auch signifikant geringer vom Verlust dokumentierten Wissens betroffen und dokumentieren zudem sowohl im Projekt als auch im Tagesgeschäft in größerem Umfang.
- **Redundanzschaffung**: [76/53] Bei der Konzeption der Studie wurde von einem Einfluss der Redundanzschaffung auf die beiden Konzepte Wissensverlust und -qualität ausgegangen, da zum einen Wissensverluste durch die stärkere Verbreitung von Wissen besser kompensierbar sind und zum anderen auch die Wissensqualität durch eine erhöhte Verfügbarkeit und Zugänglichkeit verbessert werden sollte. Dieser vermutete Einfluss in Bezug auf das Konzept Wissensqualität könnte dadurch bestätigt werden, dass fünf der sechs Variablen signifikant positiv abweichen. Dabei kommt insbesondere dem auf die Ebene Community[307] fokussierten Qualitätskriterium Anwendbarkeit von Wissen eine besondere Bedeutung zu. So kann bedingt durch die stärkere Verbreitung auf mehrere Mitarbeiter die Anwendbarkeit des Wissens verbessert werden, da der gemeinsame Kontext größer ist. Im Bereich des Konzeptes Wissensverlust wurde im Vorfeld der Studie erwartet, dass diese Maßnahme insbesondere auf die Risiken Vertretung und Nachbesetzung wirkt. Die

[307] Siehe hierzu auch Abb. 25 auf Seite 180.

Abweichungen sind in beiden Fällen zugunsten stärker steuernder Unternehmen positiv, jedoch nicht signifikant. Signifikant sind die Abweichungen bezüglich der Variable Nichtdokumentation im Projektgeschäft, wobei diese Abweichung nicht sachlogisch erklärbar ist. Analoges gilt für die drei signifikant positiven Abweichungen in Bezug auf das Konzept Wissenstransfer.

Kategorie II: Die umfassendere Implementierung der Steuerungsmaßnahmen in Kategorie II steht in Zusammenhang mit fünf bis sieben geringeren Wissensrisikoausprägungen, wobei die Dynamisierung der Zugriffsrechte, IT-Sicherheitsbewusstsein und Begrenzung der Interaktion dieser Kategorie zugeordnet werden. Die Zusammenhänge werden im Folgenden sachlogisch interpretiert.

- **Dynamisierung der Zugriffsrechte**: [59/70]: Bei der Konzeption der Studie wurde davon ausgegangen, dass die Steuerungsmaßnahme Dynamisierung der Zugriffsrechte primär auf die Wissensdiffusion und insbesondere auf die unautorisierten Zugriffe wirkt. Im Hinblick auf diese Variable besteht allerdings kein geringere Wissensrisikoausprägung. Eine signifikant geringere allerdings nicht interpretierbare Wissensrisikoausprägung betrifft die Variable Nichtdokumentation im Projektgeschäft. Weiterhin bestehen signifikant geringere Wissensrisikoausprägungen bei vier der fünf Variablen des Konzeptes Wissenstransfer sowie in Bezug auf die Variablen Korrektheit und Aktualität, die dem Konzept Wissensqualität zugeordnet sind. Für diese Wissensrisikoausprägungen besteht jedoch keine sachlogische Erklärung.
- **IT-Sicherheitsbewusstsein**: [46/83] Unternehmen mit einem höheren IT-Sicherheitsbewusstsein sind signifikant weniger durch eine Nichtdokumentation im Tagesgeschäft charakterisiert. Ein Grund könnte darin liegen, dass ein höheres Sicherheitsbewusstsein auch mit einem höheren Bewusstsein für die die Erfordernisse der Dokumentation einhergehen. In Bezug auf die positiv operationalisierten Konzepte Wissenstransfer und Wissensqualität ergeben sich ebenfalls signifikant geringere Wissensrisikoausprägungen. Im Falle des Wissenstransfers geht ein höheres Sicherheitsbewusstsein mit einem höheren Beitrag externen Wissens einher. Diese Abweichung ist allerdings nicht sachlogisch interpretierbar. In Bezug auf die Wissensqualität weichen bei der Teilstichprobe der Unternehmen mit einem höheren Sicherheitsbewusstsein die Variablen Verfügbarkeit, Rechtzeitigkeit und Korrektheit signifikant positiv ab.
- **Begrenzung der Interaktion**: [59/70] Bei der Konzeption der Studie wurde angenommen, dass diese Maßnahme insbesondere auf die beiden konträren Konzepte Wissenstransfer und -diffusion Einfluss nimmt und dabei einerseits die unerwünschte Diffusion vermindert und andererseits auch möglicherweise erwünschte Transferprozesse hemmt. Die Mittelwertabweichungen im Zusammenhang mit einer umfassenderen Begrenzung sind in Bezug auf die Wissensdiffusion weder signifikant noch eindeutig, da zwei Variablen nur gering, zwei positiv und zwei negativ abweichen. In Bezug auf den Wissenstransfer zeigt sich jedoch deutlich, dass Unternehmen, die den Wissenstransfer auf ausgewählte Mitarbeiter begrenzen, auch zugleich dessen Erfolg über alle Variablen

hinweg höher einschätzen. Dabei sind diese Abweichungen bei drei der fünf Variablen signifikant. Weiterhin bestehen zwei signifikant geringere Wissensrisikoausprägungen in Bezug auf das Konzept Wissensqualität, wobei keine sachlogischen Beziehungen zwischen dieser Steuerungsmaßnahme und dem Konzept Wissensqualität hergestellt werden können. Insgesamt ist hervorzuheben, dass der eingangs vermutete negative Einfluss auf den Wissenstransfer bedingt durch die entsprechenden Mittelwertabweichungen im Zusammenhang einer umfassenderen Implementierung nicht gegeben sein dürfte.

Kategorie III: Die umfassendere Implementierung der Steuerungsmaßnahmen Konkurrenzschutzklauseln, Geheimhaltungsvereinbarungen und Zutrittsbeschränkungen steht im Hinblick auf die 23 Wissensrisiken mit zwei bis vier geringeren Wissensrisikoausprägungen in Zusammenhang. Die Zusammenhänge in Kategorie III werden im Folgenden sachlogisch interpretiert.

- **Konkurrenzschutzklauseln**: [82/47] Im Vorfeld der Studie wurde bei der Steuerungsmaßnahme Konkurrenzschutzklauseln insbesondere eine Beeinflussung des Konzeptes Wissensdiffusion und im Speziellen in Bezug auf das Risiko der nachteiligen Mitarbeiterfluktuation vermutet. In diesem Fall besteht aber keine abweichende Wissensrisikoausprägung, die interpretiert werden könnte. In Bezug auf das Konzept Wissensverlust weichen die Wissensrisiken zur Nichtdokumentation und zum Verlust dokumentierten Wissens positiv ab, wobei keine sachlogische Interpretation angeführt werden kann. Analoges gilt für die Variable Beitrag externen Wissens.
- **Geheimhaltungsvereinbarungen**: [53/76] Im Vorfeld der Studie wurde davon ausgegangen, dass Geheimhaltungsvereinbarungen insbesondere auf die beiden Konzepte Wissensdiffusion und -transfer Einfluss haben. Während in Bezug auf die Wissensdiffusion ein positiver Einfluss erwartet wurde, wurde der Einfluss auf den Wissenstransfer indifferent gesehen, da derartige Vereinbarungen sowohl erwünschte Prozesse hemmen als auch durch verbesserte Transparenz zu einem höheren Erfolg beitragen können. In Bezug auf die Wissensdiffusion bestehen keine signifikanten Wissensrisikoausprägungen, während die Variablen Erweiterung der Wissensbasis und Beitrag externen Wissens, die dem Konzept Wissenstransfer zugeordnet sind, signifikant positiv abweichen (siehe Tab. 58). Somit kann die indifferente Sichtweise bei der Studienkonzeption nicht bestätigt werden.
- **Zutrittsbeschränkung**: [62/67] Bei der Konzeption der Studie wurde davon ausgegangen, dass Zutrittsbeschränkungen insbesondere Risiken in Bezug auf die Wissensdiffusion und den Wissensverlust beeinflussen, wobei sich auf die Variablen dieser Konzepte keine signifikanten Wissensrisikoausprägungen ergeben haben. Im Hinblick auf das Konzept Wissenstransfer sind die Risiken Beitrag externen Wissens und Qualität externen Wissens signifikant geringer ausgeprägt, wobei diese Abweichungen nicht sachlogisch interpretierbar sind. Insgesamt ist positiv anzumerken, dass die umfassendere Implementierung von Zutrittsbeschränkungen nicht mit negativen Mit-

telwertabweichungen einhergeht und somit nicht von einer Hemmung erwünschter Prozesse auszugehen ist.

Kategorie IV: Die umfassendere Implementierung der Steuerungsmaßnahmen in Kategorie IV steht mit einer bzw. keiner geringeren Wissensrisikoausprägung in Zusammenhang. Die Zusammenhänge dieser Kategorie werden im Folgenden sachlogisch interpretiert.

- **Gewerbliche Schutzechte (IPR)**: [82/47] Im Vorfeld der Studie wurde davon ausgegangen, dass gewerblich Schutzrechte primär zu einer Begrenzung von Risiken in Bezug auf die Wissensdiffusion und den Wissenstransfer führen. Insbesondere wurde ein Einfluss in Bezug auf die Variablen Imitation und Reverse Engineering vermutet. Im Hinblick auf diese beiden Variablen können zwischen den Teilstichproben nur geringe Unterschiede identifiziert werden, die nicht signifikant sind. Die einzige signifikant geringere Wissensrisikoausprägung betrifft die Variable Korrektheit von Wissen, die dem Konzept Wissensqualität zugeordnet ist. Auch diese Wissensrisikoausprägung ist nicht sachlogisch erklärbar.
- **IT-Sicherheitsrichtlinien**: [52/77] Bei der Konzeption der Studie wurde der Einfluss dieser Maßnahme insbesondere auf die Konzepte Wissensdiffusion und -verlust vermutet. Zudem kann aus der Literaturanalyse abgeleitet werden, dass potentiell erwünschte Wissenstransferprozesse durch das Erfordernis des Ergreifens zeitverbrauchender zusätzlicher Maßnahmen gehemmt werden[308]. In Bezug auf das Konzept Wissensverlust zeigt sich, dass Unternehmen, die IT-Sicherheitsrichtlinien umfassender einsetzen, geringer von Wissensverlusten betroffen sind. Im Hinblick auf Wissensverluste ist die Nichtdokumentation im Tagesgeschäft signifikant geringer ausgeprägt. Insgesamt ist positiv festzuhalten, dass IT-Sicherheitsrichtlinien nicht mit höheren Wissensrisikoausprägungen hinsichtlich der positiven Konzepte und insbesondere des Wissenstransfers in Zusammenhang stehen.
- **Zugriffsbeschränkung**: [65/64] Im Vorfeld der Studie wurde davon ausgegangen, dass die Zugriffsbeschränkung vorwiegend Einfluss auf die Konzepte Wissensdiffusion und -verlust nimmt und eine strikte Zugriffbeschränkung möglicherweise auch den Wissenstransfer hemmen könnte. Es besteht nur eine geringere Wissensrisikoausprägung in Bezug auf die Variable Reduktion von Abhängigkeiten, die dem Konzept Wissenstransfer zugeordnet ist, wobei dieser Zusammenhang allerdings nicht sachlogisch erklärt werden kann.
- **Kooperationsvereinbarungen**: [90/39] Ebenso wie bei Wissenstransferrichtlinien wird von Kooperationsvereinbarungen erwartet, dass diese Maßnahme insbesondere auf die Konzepte Wissensdiffusion und -transfer Einfluss nimmt. Diese Erwartungen können allerdings nicht bestätigt werden, da keine signifikante Wissensrisikoausprägung zu diesen sowie zu den anderen Konzepten bestehen.

[308] Siehe auch Kapitel 5.

Betrachtet man die Zusammenhänge zwischen den 13 Steuerungsmaßnahmen und den 23 Variablen, die zur Operationalisierung der Konzepte herangezogen wurden, so lassen sich folgende zentrale Erkenntnisse festhalten. Bei einer losgelösten Betrachtung der beiden positiven Konzepte Wissenstransfer und Wissensqualität fällt positiv auf, dass die umfassendere Implementierung von Steuerungsmaßnahmen mit vergleichsweise vielen geringeren Wissensrisikoausprägungen bzgl. der beiden Konzepte in Zusammenhang steht. Dabei ist insbesondere hervorzuheben, dass die beiden Maßnahmen Wissenstransferrichtlinien und Begrenzung der Interaktion entgegen der Annahmen im Vorfeld der Studie nicht mit höheren Wissensrisikoausprägungen in Zusammenhang stehen. Ebenso scheinen umfassender implementierte IT-Sicherheitsrichtlinien ebenfalls den Erfolg des Wissenstransfers nicht negativ zu beeinträchtigen.

Hinsichtlich der Konzepte Wissensdiffusion und Wissensverlust bestehen vergleichsweise weniger Zusammenhänge zwischen einer umfassenderen Implementierung der Setuerungsmaßnahmen einerseits und den geringeren Wissensrisikoausprägungen bzgl. der 23 Wissensrisiken andererseits. Bei den Risiken der Nichtdokumentation bestehen mehrere signifikant geringere Wissensrisikoausprägungen, was dadurch erklärbar ist, dass Unternehmen die stärker Steuerungsmaßnahmen ergreifen auch in umfassenderem Ausmaß Wissen dokumentieren, da das Risikobewusstsein höher ist. In Bezug auf das Risiko des Verlustes dokumentierten Wissens bestehen ebenfalls zwei signifikant geringere Wissensrisikoausprägungen. Die Wissensrisiken in Bezug auf Vertretung, Nachfolge und Reorganisation sind durch das vorhandene Set an Steuerungsmaßnahmen vergleichsweise schlecht steuerbar. Ebenso verhält es sich bei den sechs Wissensrisiken, die dem Konzept Wissensdiffusion zugeordnet sind, da bei einer stärkeren Implementierung der 13 Steuerungsmaßnahmen kein Risiko signifikant abweicht. Somit ist insbesondere bei dieser Gruppe an Risiken eine vergleichsweise schlechte Steuerbarkeit zu unterstellen.

Insgesamt ist somit positiv festzuhalten, dass keine signifikant höheren Wissensrisikoausprägungen bestehen und sich die bei der Konzeption der Studie vermuteten Austauschbeziehungen nicht bestätigt haben. Weiterhin zeigt sich, dass in Bezug auf die Wissensverluste aus Reorganisation, Nachfolge und Vertretung sowie hinsichtlich der Wissensrisiken im Kontext der Wissensdiffusion eine vergleichsweise geringe Steuerbarkeit durch das in der Studie eingeschlossene Set an Steuerungsmaßnahmen besteht. Aus diesem Grund besteht in Bezug auf diese Risiken Handlungsbedarf zur Identifikation weiterer bzw. geeigneter Steuerungsmaßnahmen. Diese Identifikation wird im Rahmen der vertiefenden Studie empirisch gestützt (siehe Abschnitte 7.5 und 7.6).

7.4 Analyse von Zusammenhängen

Zur Analyse der Zusammenhänge wird eine Clusteranalyse (7.4.2) herangezogen, die die Identifikation von Ähnlichkeiten zwischen Unternehmen und deren Zusammenfassung zu Gruppen zum Gegenstand hat. Zur Verbesserung der Qualität der Clusteranalyse wird empfohlen korrelierende Variablen auszuschließen. Dies kann durch die Bildung von Faktoren, die weitgehend voneinander unabhängig sind, erfolgen. Da die Faktorenanalyse eine Grundlage für diese Analyse darstellt wird sie im folgenden Abschnitt 7.4.1 gesondert betrachtet.

7.4.1 Faktorenanalyse

Der primäre Gegenstand der Faktorenanalyse besteht darin, aus den verwendeten Untersuchungsvariablen eine kleinere handhabbare Zahl unabhängiger Faktoren zu extrahieren und dabei den Informationsverlust so gering wie möglich zu halten. In diesem Anwendungsfall wird die Faktorenanalyse als Struktur prüfendes Verfahren eingesetzt, da theoretische Vorüberlegungen zu den Zusammenhängen bzw. zur Gruppierung der Variablen bestehen. Die Faktorenanalyse zielt insgesamt darauf ab, Faktoren zu identifizieren, die „hinter den Variablen“ stehen und sieht dabei folgendes Vorgehen vor (Johnson, Wichern 1992, 396ff; Rencher 2002, 408ff; Backhaus et al. 2006, 269ff):

(1) **Variablenauswahl und Errechnung der Korrelationsmatrix**: Im Hinblick auf die Auswahl der Variablen ist darauf zu achten, dass relevante Variablen eingeschlossen und ähnliche Variablen zusammengefasst werden. Um die Faktoren identifizieren zu können, müssen im Vorfeld die Zusammenhänge zwischen den Variablen gemessen werden. Dies erfolgt über die Korrelationsrechnung. Durch die Berechnung dieser Matrix kann augenscheinlich beurteilt werden, ob in dieser Matrix Variablencluster auftreten und die Variablen somit bündelungsfähig sind (Langer 1999, 3). Zur Überprüfung des Datensatzes auf Eignung für die Durchführung einer Faktorenanalyse können verschiedene Berechnungen, wie z.B. die Signifikanzniveaus der Korrelationen, die Inverse der Korrelationsmatrix, der Barlett-Test oder das Kaiser-Maier-Olkin-Kriterium, herangezogen werden, wobei insbesondere letztgenanntes Kriterium in der Literatur als besonders geeignetes Verfahren bezeichnet und somit präferiert wird (Backhaus et al. 2006, 269ff).

Im Kontext dieser Studie zeigt die Betrachtung der Korrelationsmatrix (siehe Tab. 95 Anhang A 4), dass die Variablen innerhalb der Konstrukte korrelieren und somit augenscheinlich Bündelungsfähigkeit besteht. Zur statistischen Beurteilung der Eignung des Datensatzes wurde zusätzlich das Kaiser-Maier-Olkin-Kriterium (KMO) zum einen für alle 36 Variablen und zum anderen auf der Ebene der einzelnen Variablen errechnet. Unter einem Wert von 0,5 ist eine Faktorenanalyse inakzeptabel, während idealerweise ein Wert von größer gleich 0,8 gute Ergebnisse erwarten lässt und daher zu präferieren ist (Backhaus et al. 2006, 276). Im vorliegenden Fall ergibt sich ein

KMO-Wert von 0,773, der im akzeptablen Bereich liegt, weshalb eine Faktorenanalyse durchgeführt werden kann.

Neben dem KMO-Wert wurde ein Anti-Image Test durchgeführt, der überprüft, inwiefern die einzelnen Variablen für eine Faktorenanalyse geeignet sind und davon ausgeht, dass sich die Varianz einer Variable in die zwei Teile Image und Anti-Image zerlegen lässt. Während sich ersterer durch die anderen Variablen erklären lässt, betrifft das Anti-Image den Teil der Varianz, der unabhängig von den anderen Variablen ist und demnach nicht erklärt werden kann. Da die Faktorenanalyse vom Zugrundeliegen von Faktoren ausgeht, sollte dieser Anteil möglichst gering sein. Demnach sollten die Werte der Diagonale der Anti-Image Korrelationsmatrix möglichst groß sein, wobei als Richtwert gilt, dass die Elemente der Diagonalen absolut mind. 75 % gegenüber den nicht auf der Diagonalen liegenden Elementen ausmachen (Backhaus et al. 2006, 275f). Die Werte der Hauptdiagonale sind wie das KMO-Kriterium zu interpretieren. In Bezug auf die 36 betrachteten Variablen liegen 13 Variablen über 0,8, 21 Variablen zwischen 0,6 und 0,8 und zwei Variablen[309] zwischen 0,5 und 0,6. Da keine Variable unter dem Schwellenwert von 0,5 liegt, ist kein Ausschluss erforderlich.

(2) **Extraktion der Faktoren und Bestimmung der Kommunalitäten**[310]: Zur Extraktion der Faktoren können verschiedene Verfahren eingesetzt werden[311], wobei im Rahmen dieser Arbeit die Hauptkomponentenanalyse eingesetzt wird, die zum Ziel hat, einen Sammelbegriff für die Variablen zu identifizieren (Backhaus et al. 2006, 289ff). Mittels dieses Verfahrens werden Faktoren ermittelt, die sukzessiv einen maximalen Anteil der Varianz beschreiben und unabhängig voneinander sind. Dabei erklärt der erste Faktor den größten Anteil der Varianz, während der zweite Faktor den zweitgrößten Anteil beschreibt. Je nach Zahl der Faktoren setzt sich dies analog fort.

(3) **Zahl der Faktoren**: Die Bestimmung der Zahl der Variablen, die im Wesentlichen der subjektiven Einschätzung unterliegt, kann durch verschiedene Kriterien gestützt werden[312], wobei im Kontext dieser Studie das Kaiser-Kriterium herangezogen wird, nach dem die Zahl der zu extrahierenden Faktoren gleich der Zahl der Faktoren mit Eigenwerten größer eins ist. Die Eigenwerte werden dabei als Summe der quadrierten Faktorladungen über alle Variablen hinweg errechnet (Backhaus et al. 2006, 295ff). Nach dem Kaiser-Kriterium lassen sich neun Faktoren extrahieren, die einen Eigenwert von >1 aufweisen (siehe Tab. 59).

[309] Dies betrifft die beiden Variablen Reverse Engineering und unerwünschter Zugang für Partner.
[310] Die Kommunalität errechnet sich aus der Summe der quadrierten Faktorladungen einer Variable und gibt an inwieweit die Varianz einer Variable durch alle Faktoren aufgeklärt wird (Backhaus et al. 2006, 289ff).
[311] Siehe hierzu auch (Johnson, Wichern 1992, 403ff).
[312] Siehe hierzu auch (Backhaus et al. 2006, 295ff).

	anfängliche Eigenwerte		Summen von quadrierten Faktorladungen für Extraktion			rotierte Summe der quadrierten Ladungen			
Komponente	gesamt	% der Varianz	kumulierte %	gesamt	% der Varianz	kumulierte %	gesamt	% der Varianz	kumulierte %
1	8,098	22,493	22,493	8,098	22,493	22,493	4,145	11,515	11,515
2	4,343	12,064	34,557	4,343	12,064	34,557	3,121	8,670	20,185
3	2,413	6,703	41,261	2,413	6,703	41,261	2,755	7,652	27,837
4	2,224	6,179	47,440	2,224	6,179	47,440	2,748	7,632	35,470
5	1,563	4,341	51,780	1,563	4,341	51,780	2,714	7,539	43,009
6	1,463	4,063	55,844	1,463	4,063	55,844	2,448	6,800	49,809
7	1,380	3,834	59,677	1,380	3,834	59,677	2,398	6,661	56,470
8	1,207	3,352	63,030	1,207	3,352	63,030	1,837	5,102	61,572
9	1,069	2,969	65,999	1,069	2,969	65,999	1,594	4,427	65,999

Tab. 59 erklärte Gesamtvarianz (ermittelt in SPSS)[313]

(4) **Faktorinterpretation**: Nach der Bestimmung der Zahl der Faktoren erfolgt eine subjektive auf inhaltlichen und theoretischen Überlegungen basierende Interpretation der Faktoren. Bei einer Einfachstruktur laden dabei die Variablen genau auf einen Faktor und werden demzufolge diesem Faktor zugeordnet. Dies ist allerdings nicht immer gegeben, da Variablen auf mehrere Faktoren laden können, weshalb eine Definition von Schwellenwerten bzw. Mindestladungen erforderlich wird. So wurde im vorliegenden Fall ein Schwellenwert von 0,5 definiert, was zur Folge hat, dass sechs Variablen ausgeschlossen wurden. Ladungen unter 0,5 sind in Tab. 60 kursiv markiert. Weiterhin wird zur verbesserten Interpretation der Faktorzuweisung vielfach Rotationen eingesetzt314, wobei im Rahmen dieser Studie von einer Unabhängigkeit der Faktoren ausgegangen und als rechtwinklige Rotation das Varimax-Verfahren verwendet wurde (Backhaus et al. 2006, 298ff). Die neun extrahierten Faktoren können den fünf Konzepten folgendermaßen zugeordnet werden. Drei Faktoren (Komponente 4, 5, 7) repräsentieren das Konzept Steuerung von Wissensrisiken, während die beiden Konzepte Wissensdiffusion (Komponente 3, 8) und Wissensverlust (Komponente 6, 9) jeweils durch zwei Faktoren repräsentiert sind. Die Konzepte Wissenstransfer (Komponente 2) und Wissensqualität (Komponente 1) werden durch je einen Faktor gemessen. Die neun Faktoren, die sich aus der in Tab. 60 dargestellten rotierten Komponentenmatrix ergeben und eine Aggregation von Variablen darstellen, können folgendermaßen interpretiert werden.

[313] Die vollständige Tabelle ist Gegenstand des Anhangs (siehe Tab. 95 in Anhang A 4)

[314] Einen detaillierten Überblick zur den verschiedenen Rotationsverfahren bieten (Johnson, Wichern 1992, 419ff; Rencher 2002, 430ff).

Variable	Abkürzung (Konzept)	Komponente								
		1	2	3	4	5	6	7	8	9
Verfügbarkeit	VERF(WQ)	,812	,112	-,054	,018	,013	-,027	,007	-,085	,156
Rechtzeitigkeit	REZT(WQ)	,788	,147	-,022	,166	,060	,007	,066	,036	,177
Nachvollziehbarkeit	NAVO(WQ)	,756	,092	,008	,012	,062	-,021	,005	-,002	,193
Aktualität	AKTU(WQ)	,665	,204	,087	,110	,236	-,139	,124	-,209	-,150
Korrektheit	KORR(WQ)	,632	,220	,007	,101	,152	-,085	,357	-,062	-,242
Anwendbarkeit	ANWE(WQ)	,616	-,036	-,083	-,015	,014	-,191	,030	,261	,110
Qualität externen Wissens	QLEW(WT)	,071	,825	,042	,150	-,036	,002	,126	-,042	,149
Quantität externen Wissens	QNEW(WT)	,181	,825	,112	,107	-,001	,040	-,028	,024	-,022
Beitrag externen Wissens	BEIT(WT)	,239	,765	-,023	,087	,212	,091	,128	,089	,134
Erweiterung der Wissensbasis	EWB(WT)	,081	,722	-,159	,086	,201	,107	,166	,172	-,023
Imitation	IMI(WD)	,007	-,182	,812	,107	-,054	,146	,118	,081	-,060
Reverse Engineering	RE(WD)	-,058	,010	,772	,052	-,123	-,085	,170	,074	,068
Competitive Intelligence	CI(WD)	-,051	,109	,695	,108	-,054	,267	-,040	,343	-,007
nacht. Mitarbeiterfluktuation	NMF(WD)	,075	,118	,657	-,079	,375	,180	-,176	,038	,113
Zugriffsbeschränkung	ZUGB(ST)	,024	,128	,103	,834	-,018	,067	,064	-,110	-,067
Begrenzung der Interaktion	BINT(ST)	,161	,095	-,172	,738	,326	,034	-,047	,141	,095
Dyn. der Zugriffsrechte	DYNZ(ST)	,129	,172	,153	,593	,262	-,013	,217	,026	,055
Kooperationsvereinbarungen	KOV(ST)	,006	,022	,123	,485	,227	,099	,226	,224	,180
Zutrittsbeschränkung	ZUTB(ST)	,011	,177	,243	,426	,343	,002	,270	-,259	,065
Wissenstransferrichtlinien	WTRL(ST)	,270	,043	-,072	,215	,678	,025	,223	,112	,253
Geheimhaltungsvereinbarungen	GHVB(ST)	,151	,240	-,108	,161	,655	-,106	,129	-,067	,219
gewerbliche Schutzrechte (IP)	IPR(ST)	-,077	,015	,081	,204	,555	-,013	,477	,204	-,153
Klassifikation von Wissen	KLASS(ST)	,389	,101	,119	,285	,526	-,103	,088	-,031	,029
Konkurrenzschutzklauseln	KOS(ST)	,007	,061	-,281	,355	,460	,112	,345	,294	,125
Vertretung	VER(WV)	-,078	,098	,132	-,022	-,009	,864	,008	-,010	-,053
Nachbesetzung	NAB(WV)	-,016	,171	,063	,067	,068	,795	,080	,119	-,286
Reorganisation	REO(WV)	-,294	-,100	,164	,155	-,120	,676	-,112	,150	,272
Verlust dok. Wissens	VDW(WV)	-,407	-,088	,034	-,017	-,167	,442	-,276	,230	,158
IT-Sicherheitsrichtlinien	ITSR(ST)	,084	,138	,045	,183	,161	-,028	,732	-,040	,259
IT-Sicherheitsbewusstsein	ITSB(ST)	,223	,154	,114	,136	,208	,007	,723	-,077	,044
Redundanzschaffung	REDU(ST)	,240	,308	-,003	-,020	,210	-,127	,366	,329	,178
unautorisierte Zugriffe	UZU(WD)	-,081	,049	,300	-,007	,136	,111	-,060	,708	-,054
unerw. Zugang für Partner	UZP(WD)	-,062	,190	,331	,079	,004	,320	-,021	,586	-,049
Reduktion der Abhängigkeit	REAB(WT)	,214	,098	-,050	,424	-,269	-,052	,392	,437	-,028
Nichtdokumentation (PG)	NDPG(WV)	-,250	-,222	-,057	-,136	-,225	,076	-,128	,049	-,718
Nichtdokumentation (TG)	NDTG(WV)	-,414	-,086	-,046	-,025	-,219	,084	-,234	,033	-,579

Tab. 60 rotierte Komponentenmatrix (ermittelt in SPSS)

- **Steuerung I: „Begrenzung des Zugangs“** (Komponente 4)**:** Der erste Faktor, der das Konzept der Steuerung von Wissensrisiken repräsentiert, schließt die Variablen Zugriffsbeschränkung, Begrenzung der Interaktion und Dynamisierung der Zugriffsrechte ein und kann zusammenfassend als „Begrenzung des Zugangs“ bezeichnet werden. Diese Benennung kann auch dadurch gestärkt werden, dass auch die thematisch verwandten Zutrittsbeschränkungen auf diesen Faktor laden, allerdings aufgrund ihrer Ladung unter dem Schwellenwert von 0,5 ausgeschlossen werden.
- **Steuerung II: „Kontrolle der Weitergabe“** (Komponente 5): Der zweite Faktor, der dem Konzept Steuerung von Wissensrisiken zuzuordnen ist, schließt die Variablen Wissenstransferrichtlinien, Geheimhaltungsvereinbarungen, gewerbliche Schutzrechte und Klassifikation von Wissen ein und ist im Vergleich zum Faktor „Begrenzung des Zugangs“ stärker unternehmensextern fokussiert. Die Klassifikation von Wissen stellt in diesem Zusammenhang eine Voraussetzung zur kontrollierten Weitergabe dar. Aus diesem Grund wird dieser Faktor als „Kontrolle der Weitergabe“ bezeichnet. Auch die Variable Konkurrenzschutzklauseln, die aufgrund ihrer zu geringen Faktorladung ausgeschlossen wurde, lädt am stärksten auf diesen Faktor und kontrolliert ebenfalls die Weitergabe von Wissen.
- **Steuerung III: „IT-Sicherheit“** (Komponente 7): Die beiden Variablen IT-Sicherheitsrichtlinien und IT-Sicherheitsbewusstsein werden zu einem Faktor zusammengefasst, der ebenso das Konzept Steuerung von Wissensrisiken repräsentiert. Dieser Faktor wird aufgrund der Gemeinsamkeiten der einbezogenen Variablen nachfolgend als „IT-Sicherheit“ bezeichnet.
- **Wissensverlust I: „fluktuationsbedingter Wissensverlust“** (Komponente 6): Das Konzept Wissensverlust, das durch zwei Faktoren repräsentiert wird, schließt im ersten Faktor die Variablen Vertretung, Nachbesetzung und Reorganisation ein. Diese drei Variablen, die inhaltlich verwandt sind, stellen auf Wissensverluste ab, die sich aus einer Intra-, Inter- und Extrafluktuation ergeben. Demzufolge wird dieser Faktor als „fluktuationsbedingter Wissensverlust“ bezeichnet.
- **Wissensverlust II: „Nichtdokumentation“** (Komponente 9): Der zweite Faktor, der das Konzept Wissensverlust repräsentiert, fasst die beiden Variablen zur Nichtdokumentation von Wissen im Projekt- und Tagesgeschäft zusammen. Somit werden diese Teilaspekte nachfolgend aggregiert betrachtet und der Faktor als „Nichtdokumentation“ bezeichnet.
- **Wissensdiffusion I: „wettbewerbsbedingte Wissensdiffusion“** (Komponente 3): Das Konzept Wissensdiffusion wird ebenfalls durch zwei Faktoren repräsentiert. Der erste Faktor fasst die Variablen Imitation, Reverse Engineering, Competitive Intelligence und nachteilige Mitarbeiterfluktuation zusammen. Dabei wird ersichtlich, dass die ersten drei Variablen durch externe Akteure und insbesondere Wettbewerber verursacht werden, da diese gezielt Produkte des Unternehmens imitieren, Wissen destillieren oder sensitive Informationen über das Unternehmen sammeln. Auch die nachteilige Mitarbeiterfluktuation kann unternehmensextern z.B. durch Abwerbung verursacht

sein. Aus diesem Grund wird dieser Faktor nachfolgend als „wettbewerbsbedingte Wissensdiffusion“ bezeichnet und stellt vorwiegend auf Aktivitäten ab, die von Wettbewerbern ausgehen.

- **Wissensdiffusion II: „zusammenarbeitsbedingte Wissensdiffusion“** (Komponente 8): Der zweite Faktor zur Wissensdiffusion schließt die beiden Variablen unautorisierte Zugriffe und unerwünschter Zugang des Partners ein. Im Vergleich zum ersten Faktor zur Wissensdiffusion ist dieser Faktor allgemeiner ausgerichtet und stellt auf den Zugang und Zugriff ab, der im Rahmen der Zusammenarbeit verursacht wird. Abgrenzend zu der wettbewerberfokussierten Ausrichtung des Faktors I, wird der unerwünschte Zugang der Partner aufgrund der Zusammenarbeit eher unternehmensintern betrachtet. Aus diesem Grund wird dieser Faktor als „zusammenarbeitsbedingte Wissensdiffusion“ bezeichnet.
- **Wissenstransfer** (Komponente 2): Das Konzept Wissenstransfer wird durch einen Faktor repräsentiert, der mit Ausnahme der Variable Reduktion der Abhängigkeit vom Wissen des Partners alle Variablen einschließt, die bei der Konzeption der Studie zur Operationalisierung herangezogen wurden. Somit werden die Variablen Erweiterung der Wissensbasis, Beitrag externen Wissens, Qualität und Quantität externen Wissens zu einem Faktor zusammengefasst, der nachfolgend als „Wissenstransfer“ bezeichnet wird. Die Variable Reduktion von Abhängigkeiten lädt mit 0,098 allerdings nur sehr gering auf diesen Faktor.
- **Wissensqualität** (Komponente 1): Analog zum Wissenstransfer wird auch das Konzept Wissensqualität durch einen Faktor repräsentiert, der die Variablen Verfügbarkeit, Rechtzeitigkeit, Nachvollziehbarkeit, Aktualität, Korrektheit und Anwendbarkeit einschließt. Dieser Faktor umfasst somit alle sechs zur Operationalisierung herangezogenen Variablen ein und wird daher allgemein als „Wissensqualität“ bezeichnet.

  Sechs Variablen wurden aufgrund der zu geringen Faktorladung von $\leq 0{,}5$ ausgeschlossen. Dabei würden die Variablen Kooperationsvereinbarungen und Zutrittsbeschränkung am ehesten auf den Faktor „Begrenzung des Zugangs“ mit 0,48 bzw. 0,42 laden, während die ausgeschlossene Variable Konkurrenzschutzklauseln mit 0,46 auf den Faktor „Kontrolle der Weitergabe“ lädt. Die Variable Verlust dokumentierten Wissens wäre dem Faktor „fluktuationsbedingter Wissensverlust“ zuzuordnen und die Variable Redundanzschaffung dem Faktor „IT-Sicherheit“, da sie auf diese Faktoren mit 0,44 bzw. 0,36 laden. In beiden Fällen ist unabhängig von der zu geringen Faktorladung keine sachlogisch sinnvolle Interpretation möglich. So passt die Variable Redundanzschaffung inhaltlich nicht zum Faktor „IT-Sicherheit“, entstammt allerdings demselben Konzept. Die Reduktion der Abhängigkeit lädt mit 0,43 am stärksten auf den Faktor „zusammenarbeitsbedingte Wissensdiffusion“. Betrachtet man diese Zuordnung unabhängig des Schwellenwertes der Faktorladung so würde bei Einbezug der Variable eine Vermengung der zwei konträren Konzepte Wissenstransfer und -diffusion erfolgen.

(5) **Bestimmung der Faktorwerte**: Neben der Auswahl der Faktoren ist auch die Bestimmung der Faktorwerte z.B. für weitere Berechnungen wie die Clusteranalyse erforderlich (Johnson, Wichern 1992, 429f; Backhaus et al. 2006, 302ff). Die Faktorwerte wurden im vorliegenden Fall als neue Variablen in SPSS unter Verwendung der Regression als Berechnungsmethode gespeichert und werden für die weiteren multivariaten Auswertungen herangezogen.

Vergleicht man diese Faktoren mit dem ursprünglichen Modell zur Operationalisierung (siehe 6.3.2), das zur Konzeption der Studie herangezogen wurde, so ist das Modell insbesondere im Hinblick auf die beiden Konzepte Wissenstransfer und Wissensqualität als hoch valide zu bewerten, da die Faktoren nahezu dem Ausgangsmodell entsprechen. Die Konzepte Wissensdiffusion und Wissensverlust werden durch je zwei Faktoren repräsentiert, deren inhaltliche Nähe auch bei der Konzeption des Ausgangsmodells ersichtlich ist. Die Repräsentation des Konzeptes Steuerung durch drei Faktoren erhöht die Aussagekraft deutlich, da eine Zusammenfassung von 13 Einzelvariablen aufgrund der großen Unterschiede schwer ist. Insgesamt liegt in Bezug auf die beiden Konzepte Wissenstransfer und Wissensqualität eine hohe Konstruktvalidität vor, da eine starke Deckungsgleichheit der Faktoren mit dem Ausgangsmodell vorliegt. Die Variablen der anderen drei Konzepte werden zu jeweils zwei oder drei Faktoren zusammengefasst, weshalb keine vollständige Bestätigung des Ausgangsmodells und somit eine geringere Validität vorliegt.

7.4.2 Clusteranalyse

Nachfolgender Abschnitt fokussiert auf die Analyse von Ähnlichkeiten zwischen den in die Stichprobe eingeschlossenen Unternehmen. Zu diesem Zweck wird eine Clusteranalyse durchgeführt, wobei zunächst in Abschnitt 7.4.2.1 die Ziele und das allgemeine Vorgehen beschrieben werden und in Abschnitt 7.4.2.2 die Durchführung und die Interpretation erörtert werden. Im Anschluss daran werden in Abschnitt 7.4.2.3 vertiefenden Fragestellungen zu den einzelnen Clustern abgeleitet, die daraufhin mit ausgewählten Ansprechpartnern, deren Unternehmen das jeweilige Cluster besonders gut repräsentierten, in Abschnitt 7.5 detailliert analysiert werden.

7.4.2.1 Ziele, Vorgehen und Vorüberlegungen

Nach der deskriptiven Auswertung der einzelnen Konzepte sollen im Folgenden Zusammenhänge zwischen den an der Studie teilnehmenden Unternehmen entdeckt werden. Zu diesem Zweck wird eine Clusteranalyse herangezogen. Diese hat zum Ziel, die heterogenen Objekte einer Stichprobe in Abhängigkeit ausgewählter Variablen auf der Basis multivariater Prozeduren in möglichst homogene Gruppen einzuteilen. Derartige Analysen haben ein breites Anwendungsfeld, wobei die zentrale Herausforderung darin besteht, aus einer Vielzahl möglicher Lösungen die „wahren“ Zusammenhänge zu

identifizieren. Allgemein sieht die Clusteranalyse folgendes methodisches Vorgehen vor (Johnson, Wichern 1992, 573ff; Rencher 2002, 451ff; Backhaus et al. 2006, 492ff).

(1) **Bestimmung der Ähnlichkeiten**: In einem ersten Schritt werden dabei die Ähnlichkeiten durch Proximitätsmaße bestimmt, die sich jeweils auf zwei Objekte beziehen. Im Kontext dieser Studie wird aufgrund der weiten Verbreitung die quadrierte euklidische Distanz[315] als Proximitätsmaß zugrunde gelegt. Sie wird dadurch gebildet, dass zwischen zwei Objekten je Variable die betragsmäßige Differenz gebildet, quadriert und aufsummiert wird (Backhaus et al. 2006, 493ff). Im vorliegenden Fall betrifft diese Distanzbildung die 37 Likert skalierten Variablen[316]. Im Ergebnis führt diese Berechnung zu einer Distanzmatrix, die in den Zellen jeweils die Distanz zwischen zwei Objekten angibt und die Grundlage für die Fusionierung bildet.

(2) **Auswahl des Fusionierungsalgorithmus**: Auf dieser Basis werden die einzelnen Objekte so zu Gruppen zusammengefasst, dass sie im Hinblick auf die einbezogenen Variablenausprägungen möglichst gut übereinstimmen, wobei die Fusionierung solange erfolgt, bis alle Objekte einer Gruppe zugewiesen sind. Zur Fusionierung besteht eine Vielzahl an Algorithmen[317], wobei in dieser Studie aufgrund ihrer Verbreitung hierarchisch agglomerative und als spezieller Algorithmus dieser Kategorie das Ward Verfahren herangezogen wird, nach dem die Zunahme der Varianz beim Vereinigen der Cluster das Zuweisungskriterium darstellt (Rencher 2002, 455ff)[318]. Das Ward Verfahren kann als besonders guter Fusionierungsalgorithmus angesehen werden, wenn als Voraussetzung die Anwendung eines Distanzmaßes inhaltlich sinnvoll ist, metrische Skalierung vorliegt, Ausreißer ausgeschlossen wurden und die Variablen unkorreliert sind (Bortz 2005, 573; Backhaus et al. 2006, 510ff, 528). Diese Anforderungen sind erfüllt und werden nach der Beschreibung des allgemeinen Vorgehens gesondert erläutert.

(3) **Bestimmung der Clusterzahl**: Basierend auf der mehrstufigen Zuweisung durch den Fusionierungsalgorithmus gilt es, die ideale Zahl an Gruppen zu definieren, wobei im Hinblick auf die Clusteranzahl ein Zielkonflikt zwischen Handhabbarkeit und Homogenität besteht. Erstere wird dabei durch eine geringe Anzahl an Clustern verbessert, während Homogenität eher bei einer größeren Clusteranzahl sichergestellt werden kann. Dabei sollte die Clusterzahl auf statistischen Kriterien und nicht auf sachlogischen Überlegungen basieren (Backhaus et al. 2006, 534ff).

Zur Verbesserung der Ergebnisse der Clusteranalyse werden in der einschlägigen Literatur Empfehlungen abgegeben, die nachfolgend erläutert und im Kontext des zugrunde liegenden Datensatzes diskutiert werden (Backhaus et al. 2006, 549). Diese Empfehlungen betreffen Maßnahmen, die im Vor-

[315] Alternative Maße sind die City-Block Metrik, die Mahalanobis-Distanz und der Q-Korrelationskoeffizient.
[316] Siehe auch 6.3.2.
[317] Siehe hierzu auch (Johnson, Wichern 1992, 584ff).
[318] Weitere Fusionierungsalgorithmen zur Berechnung der Distanz zwischen den Clustern sind z.B. das Single bzw. Complete Linkage, das den minimalen bzw. maximalen Abstand zweier Objekte aus den beiden Clustern zugrunde legt (Rencher 2002, 455ff).

feld der Clusteranalyse durchgeführt werden sollten, um die Qualität der Fusionierung (siehe 2) zu verbessern.

a) **Relevanz der berücksichtigten Variablen:** Die erste Anforderung besteht darin, dass nur Variablen einbezogen werden, die für den Untersuchungsgegenstand von Relevanz sind (Backhaus et al. 2006, 549). Hinsichtlich der 37 Likert skalierten Variablen, die den Gegenstand der Studie darstellen, sind nach inhaltlichen Überlegungen keine Variablen auszuschließen, da sowohl die einzelnen Risiken als auch die Steuerungsmaßnahmen für eine Gruppierung der Objekte von Relevanz sind.

b) **Ausschluss konstanter Merkmale**: Neben nicht relevanten Variablen, sind auch solche auszuschließen, die für alle Merkmalsträger den gleichen oder nahezu gleichen Wert annehmen, da sie keine Trennungskraft aufweisen und daher die Fusionierung zu Verzerrungen führen kann (Backhaus et al. 2006, 550). Von den 37 Likert skalierten Variablen wird die Variable Bedeutung der Ressource Wissen ausgeschlossen, da der korrespondierenden Aussage 82% der Unternehmen stark oder sehr stark zugestimmt haben, was sich auch in einem vergleichsweise hohen Mittelwert von 6,01 zeigt. Der hohe Mittelwert und schiefe Verteilung deutet auf Konstanz hin, was zur Folge hat, dass die Trennkraft der Variable zu gering ist, um deren Einschluss zu rechtfertigen.

c) **Ausschluss stark korrelierender Variablen**: Variablen, die stark korreliert sind, gehen mit einem höheren Gewicht in die Clusteranalyse ein und können somit zu Verzerrungen führen, da bei der Fusionierung mehrere Variablen überbetont werden. Im Hinblick auf die Qualität der Zuordnung sollten demnach stark korrelierte Variablen ausgeschlossen werden, da sie durch die andere Variable miterfasst werden und somit redundant sind (Backhaus et al. 2006, 549). Betrachtet man die Korrelationsmatrix (siehe Tab. 95 Anhang A 4) so bestehen vielfach Korrelationen zwischen den einzelnen Variablen, die primär innerhalb der Konzepte auftreten. Bedingt durch diese Korrelationen werden die Ergebnisse der in Abschnitt 7.4.1 durchgeführten Faktorenanalyse zugrunde gelegt, die die 36 Likert skalierten Variablen zu neun Faktoren, die weitgehend voneinander unabhängig sind, zusammenfasst.

d) **Eliminierung von Ausreißern**: Zur Verbesserung der Fusionierung sollen als weitere Anforderung Ausreißer, also Objekte, die sich stark von den übrigen Objekten unterscheiden, eliminiert werden. Dies ist erforderlich, da der Einbezug dieser Merkmalsträger den Fusionierungsprozess negativ beeinträchtigt und so das Erkennen der Zusammenhänge erschwert wird. Zum Ausschluss von Ausreißern kann das Single Linkage Verfahren herangezogen werden. Dabei werden die minimalen Abstände zwischen den Objekten betrachtet, wobei die Prämisse zugrunde liegt, dass jedes Objekt eine Gruppe darstellt. Auf dieser Basis werden Objekte solange zusammengefasst bis alle Objekte zugeordnet sind. Die Objekte, die am Schluss zugewiesen werden, weisen die größten Abstände bzw. Unterschiede auf, sind dabei am unähnlichsten zu allen anderen Gruppen und kön-

nen daher zu Verzerrungen führen (Johnson, Wichern 1992, 589f; Backhaus et al. 2006, 549). Im Rahmen dieser Studie wurden auf der Basis des Dendogramms sechs Objekte identifiziert, die vergleichsweise schwer zuweisbar sind und daraufhin ausgeschlossen, wodurch sich die Stichprobe auf 123 Unternehmen reduziert.

7.4.2.2 Bestimmung der Clusterzahl

Insgesamt bestehen bei der Wahl der Clusteranzahl verschiedene Zielsetzungen, die es miteinander zu vereinbaren gilt. Die zentrale Anforderung besteht in der Gewährleistung der Trennschärfe und somit darin, dass die jeweiligen Objekte eines Clusters möglichst homogen zueinander und möglichst heterogen zu den Objekten der anderen Cluster sind. Zudem sollte die Clusterlösung möglichst gut interpretierbar sein, wobei die Interpretierbarkeit mit zunehmender Clusteranzahl erschwert wird. Dies ist darauf zurückzuführen, dass die Cluster, die in Bezug auf die neun Faktoren keine Extremwerte annehmen, vielfach aufgrund geringer Mittelwertabweichungen schwerer zu interpretieren. Da die Abstände zwischen den Clustern abnehmen, kann dann das Kriterium der Trennschärfe und der guten Interpretierbarkeit vergleichsweise schlechter erfüllt werden. Letztlich muss die Clusterlösung stabil sein und die Zuweisung der Objekte bei der Wahl unterschiedlicher Fusionierungsalgorithmen Ähnlichkeiten aufweisen. Vor dem Hintergrund dieser verschiedenen Anforderungen werden nachfolgend die Clusterzahl bestimmt und die Charakteristika der Cluster näher beschrieben.

Die Bestimmung der Clusterzahl kann durch das Ellbogenkriterium gestützt werden. Dabei werden die Fehlerquadratsumme und die Clusterzahl in einem Koordinatensystem gegeneinander abgetragen, wobei sich bei den größten Heterogenitätssprüngen der Ellbogen, also ein Knick im Graphen, zeigt (Backhaus et al. 2006, 534ff). Bedingt durch die hohe Zahl der Objekte führt die Verwendung des Ellbogenkriteriums zu keiner eindeutigen Lösung, weshalb nachfolgend das Dendogramm (siehe Abb. 39), in dem die einzelnen Schritte der Fusionierung zusammengefasst sind, herangezogen wird. Ausgehend von einer 8-Clusterlösung sind die Clustergrößen vergleichsweise homogen und weisen eine Spannweite von neun bis 23 Objekte auf. Bei hierarchisch agglomerativen Verfahren wird unterstellt, dass jedes Objekt ein Cluster darstellt und auf dieser Basis die einzelnen Objekte zusammengefasst. Im konkreten Fall würden bei einer 2-Clusterlösung zwei homogene Cluster mit 61 bzw. 62 Unternehmen verbleiben (siehe Abb. 39). Die Homogenität bei den Zwischenlösungen mit drei bis sieben Clustern ist vergleichsweise gering, da sich Cluster eins ab einer 3-Clusterlösung deutlich abhebt und in jedem Schritt neun Unternehmen einschließt.

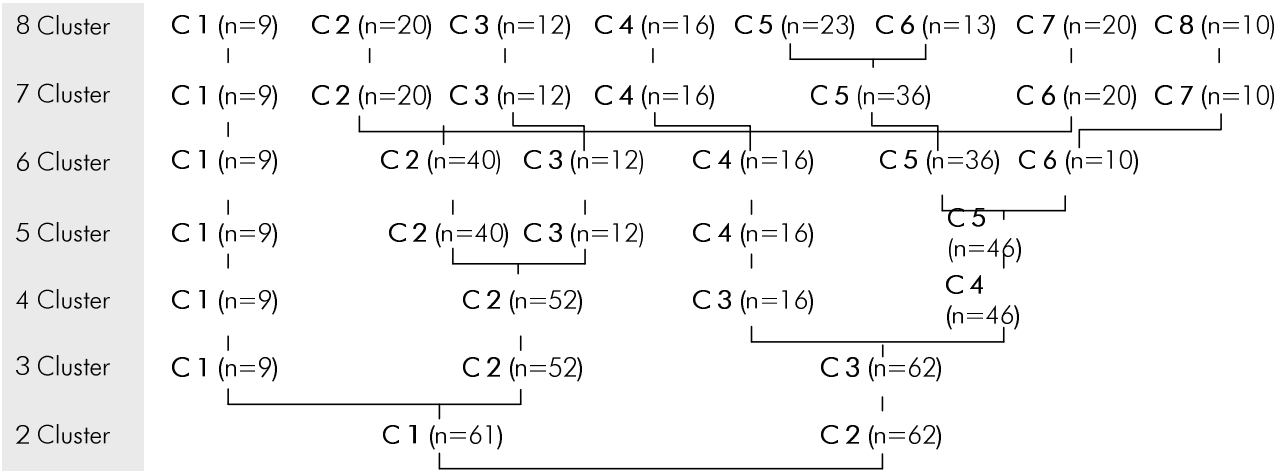


Abb. 39 Clustergrößen bei 2- bis 8-Clusterlösungen

Dadurch bedingt, dass die Unterschiede zwischen den Clustern, die im Hinblick auf die einbezogenen Faktoren keine Extremwerte annehmen, gering sind, nimmt die Interpretierbarkeit der Clusterlösung mit zunehmender Clusterzahl ab. Zudem nimmt mit zunehmender Clusteranzahl die Spannweite aus Minima und Maxima zu, da die Heterogenität der Cluster zueinander ansteigt. Andererseits sind die mittleren Cluster vergleichsweise schwerer interpretierbar und liegen in Bezug auf die Mittelwertdifferenzen enger beisammen. Aufgrund der zum Teil geringen Unterschiede werden Clusterlösungen mit sechs oder mehr Clustern von der weiteren Betrachtung ausgeschlossen. Eine 2-Clusterlösungen fasst zu heterogene Objekte zusammen und wird ebenfalls ausgeblendet. Demnach wird im Folgenden eine Entscheidung zwischen einer 3-, 4- oder 5-Clusterlösung getroffen. Bezüglich der Interpretierbarkeit der verschiedenen Lösungen besteht das Ziel darin, eine Lösung mit möglichst trennscharfen Clustern zu identifizieren. Zu dieser Beurteilung wird nachfolgend die Differenz der minimalen und maximalen Mittelwerte über die jeweiligen Cluster hinweg herangezogen.

Clusterzahl / Faktor	3	4	5
Steuerung I	1,06	1,41	1,66
Steuerung II	0,20	1,06	1,06
Steuerung III	0,59	0,81	0,91
Wissensverlust I	0,75	1,31	1,80
Wissensverlust II	0,24	0,25	0,39
Wissensdiffusion I	2,13	2,25	2,25
Wissensdiffusion II	1,28	1,38	1,38
Wissenstransfer	1,44	1,44	1,49
Wissensqualität	1,37	1,37	2,15

Tab. 61 Spannweite der Mittelwerte

Betrachtet man die in Tab. 61 dargestellten Differenzen der minimalen und maximalen Mittelwerte je Faktor, so zeigt sich, dass bei einer 3-Clusterlösung die Faktoren Steuerung II, Steuerung III und Wissensverlust I nur gering abweichen und eine Spannweite zwischen 0,2 und 0,59 aufweisen. Somit sind die Unterschiede in Bezug auf die beiden Faktoren kaum interpretierbar. Bei einer 4-Clusterlösung sind nur noch die Abweichungen in Bezug auf den Faktor Wissensverlust II gering variierend. Dies trifft auch auf die 5-Clusterlösung zu, die bei den anderen Faktoren eine höhere Differenz aufweist. Dabei ist die Zunahme der Differenz zwischen minimaler und maximaler

Ausprägung der Faktoren bei der 5-Clusterlösung in der Relation zur Veränderung zwischen der 3- und 4-Clusterlösung vergleichsweise geringer. Die 5-Clusterlösung hat zudem zum Problem, dass sich die Faktoren, die jeweils zwischen den Extremen liegen, vergleichsweise schwerer abgrenzen lassen und die Trennschärfe zwischen den mittleren Clustern geringer ist. Aus diesem Grund wird eine 4-Clusterlösung herangezogen. Entsprechend dieser Lösung bestehen zwei kleinere Cluster mit neun bzw. 16 Unternehmen und zwei größere Cluster mit 52 bzw. 46 Unternehmen. Vergleicht man diese Lösung mit dem Ergebnis anderer Fusionierungsalgorithmen wie dem Complete Linkage Verfahren so sind die Cluster I und III stabil, während die Cluster II und IV vergleichsweise weniger einheitlich zusammengesetzt sind.

7.4.2.3 Interpretation der Cluster und Ableitung vertiefender Fragestellungen

Nachdem die Clusteranzahl bestimmt wurde erfolgt in diesem Abschnitt die Interpretation der einzelnen Cluster sowie die Ableitung vertiefender Fragestellungen, deren Analyse Gegenstand von Abschnitt 7.5 ist.

Bezogen auf die in Abb. 39 dargestellte Zusammenfassung der Cluster dürften insbesondere die Charakteristika des Clusters I von Interesse sein, da dieses Cluster über die verschiedenen Lösungen hinweg vergleichsweise konstant ist und sich daher stark von den anderen Gruppen abzuheben scheint. Betrachtet man die Ausprägung der Faktoren über die 4-Clusterlösung hinweg, so ergeben sich die in Tab. 62 abgetragenen Werte. Diese liegen der nachfolgenden detaillierten Betrachtung der Cluster zugrunde. Dabei sind die Werte in Tab. 62 als Abweichung vom Mittelwert zu sehen, wobei dieser bedingt durch Verwendung von Faktoren für die Clusteranalyse auf den Wert 0 normiert ist.

Cluster	**I**	**II**	**III**	**IV**	**Δ**
n / **Faktor**	**9**	**52**	**16**	**46**	
Steuerung I	0,82	-0,24	-0,59	0,44	1,41
Steuerung II	0,13	-0,07	-0,83	0,23	1,06
Steuerung III	0,15	-0,26	0,55	0,24	0,81
Wissensverlust I	0,59	-0,15	-0,72	0,23	1,31
Wissensverlust II	-0,17	-0,04	0,08	0,07	0,25
Wissensdiffusion I	1,55	0,48	-0,23	-0,70	2,25
Wissensdiffusion II	1,06	0,07	0,06	-0,32	1,38
Wissenstransfer	0,81	-0,62	0,81	0,25	1,44
Wissensqualität	1,05	-0,31	0,37	-0,13	1,37

Tab. 62 Ausprägung der Faktoren bei vier Clustern

Cluster I: Cluster I ist dadurch charakterisiert, dass die Steuerung vergleichsweise höher ist, wobei insbesondere die Begrenzung des Zugangs hoch ausgeprägt ist und die Kontrolle der Weitergabe sowie die IT-Sicherheit im Vergleich zu den anderen Clustern dem Durchschnitt entsprechen. Unternehmen in diesem Cluster sind zudem dadurch charakterisiert, dass sie im Vergleich zu Unternehmen anderer Cluster vergleichsweise stärker von fluktuationsbedingten Wissensverlusten betroffen sind bzw. diese Risiken höher einschätzen. Risiken in Bezug auf die Nichtdokumentation, sind in diesem Cluster am geringsten ausgeprägt, wobei diese Abweichung bedingt durch die geringe Differenz von 0,25 zwischen dem minima-

len und maximalen Mittelwert über alle Cluster hinweg nahezu nicht interpretierbar ist. Unternehmen in Cluster I sind zudem am stärksten von den Risiken einer unerwünschten Wissensdiffusion betroffen. So werden sowohl die wettbewerbs- als auch die zusammenarbeitsbedingte Wissensdiffusion in diesen Unternehmen am höchsten eingeschätzt. Im Hinblick auf die beiden positiven Konzepte Wissenstransfer und Wissensqualität werden sowohl der Erfolg des Wissenstransfers als auch das Niveau der Qualität im Vergleich zu den anderen Clustern am höchsten eingeschätzt. Insgesamt sind Unternehmen in diesem Cluster von einer positiveren Ausprägung der beiden positiven Konzepte und einer jeweils negativeren Ausprägung der beiden negativen Konzepte charakterisiert, wobei der Faktor Nichtdokumentation nicht interpretiert werden kann.

Cluster II: Unternehmen in Cluster II sind dadurch charakterisiert, dass die Steuerung über alle drei Faktoren hinweg im Vergleich zu den anderen Clustern ausgehend vom Mittelwert negativ abweicht, was auch als vergleichsweise geringere Steuerung zu interpretieren ist. Die IT-Sicherheit ist am geringsten ausgeprägt. Im Hinblick auf Wissensverluste sind Unternehmen in Cluster II vergleichsweise geringer betroffen, wobei der Faktor, wie auch bei Cluster I schon erwähnt, nicht interpretiert werden kann. Risiken in Bezug auf die unerwünschte Diffusion liegen verglichen mit den anderen Clustern ebenenfalls im Durchschnitt, wobei die wettbewerbsbedingte Wissensdiffusion vergleichsweise stärker ausgeprägt ist. Die beiden Faktoren Wissenstransfer und Wissensqualität weisen in der Relation zu den anderen Clustern im Hinblick auf den Erfolg bzw. das Qualitätsniveau die niedrigsten Werte auf. Insgesamt sind Unternehmen in diesem Cluster in der Relation zu den anderen Clustern durch eine geringere Steuerung charakterisiert und weisen zudem den geringsten Wissenstransfererfolg und das niedrigste Niveau der Wissensqualität auf, wobei die negativ operationalisierten Konzepte im Durchschnitt liegen.

Cluster III: Bezogen auf das Konzept Steuerung begrenzen Unternehmen in Cluster III vergleichsweise am geringsten den Zugang und kontrollieren die Weitergabe des Wissens am geringsten. Demgegenüber ist die IT-Sicherheit in diesem Cluster am höchsten ausgeprägt. Bezüglich des Konzeptes Wissensverlust ist Cluster III dadurch charakterisiert, dass die fluktuationsbedingten Wissensverluste am geringsten eingeschätzt werden. Die Risiken der Nichtdokumentation werden in der Relation zu den anderen Clustern am höchsten eingeschätzt, wobei auch hier die geringe Differenz zwischen dem minimalen und maximalen Mittelwert die Interpretierbarkeit dieses Faktors verhindert. Die Risiken in Bezug auf die wettbewerbs- und zusammenarbeitsbedingten Wissensdiffusion werden durchschnittlich eingeschätzt, wobei erstgenannter Faktor eine vergleichsweise geringere Risikoausprägung aufweist. Der Wissenstransfererfolg wird ebenso wie in Cluster I vergleichsweise hoch eingeschätzt. Die Beurteilung des Niveaus der Wissensqualität weist ausgehend vom Mittelwert eine vergleichsweise positive Einschätzung auf. Insgesamt ist die Steuerung in diesem Cluster im Vergleich zu den anderen

Clustern geringer, wobei zugleich die fluktuationsbedingten Wissensverluste am geringsten und der Wissenstransfererfolg vergleichsweise hoch eingeschätzt werden.

Cluster IV: Unternehmen in diesem Cluster ergreifen in der Relation umfassender Steuerungsmaßnahmen, wobei die Kontrolle der Weitergabe im Vergleich zu den anderen Clustern am höchsten ausgeprägt ist. Die Risiken in Bezug auf fluktuationsbedingte Wissensverluste und Nichtdokumentation werden von den Unternehmen in diesem Cluster in der Relation zu den anderen Clustern durchschnittlich eingeschätzt. Demgegenüber werden Risiken der wettbewerbs- und zusammenarbeitsbedingten Wissensdiffusion im Vergleich zu den anderen Clustern am geringsten eingeschätzt. Der Erfolg des Wissenstransfers und das Niveau der Wissensqualität entsprechen in etwa dem Durchschnitt. Insgesamt fällt bei Unternehmen dieses Clusters auf, dass sie am geringsten von den Risiken der Wissensdiffusion betroffen zu sein scheinen. Neben der Analyse der konkreten Ausprägungen der Faktoren über die vier Cluster hinweg, ist auch die Zusammensetzung der Cluster in Bezug auf die Charakteristika Unternehmensgröße, Brachenzugehörigkeit sowie implementierte RM- und WM- Initiativen von Relevanz. Analysiert man die Zusammenhänge zwischen Clusterzuordnung und Mitarbeiterzahl (Tab. 63) so ergeben sich Abweichungen von einer proportionalen Verteilung insbesondere bei der Größenklasse Großunternehmen. So sind in Cluster II fünf Großunternehmen weniger zugeordnet, während in Cluster III drei und Cluster IV vier Großunternehmen mehr als bei einer proportionalen Verteilung zugewiesen sind.

			I	II	III	IV
MA/n	**n=129**	**n=123**	**n=9**	**n=52**	**n=16**	**n=46**
0-9	12	11	1	5	0	5
10-49	12	12	1	8	1	2
50-249	83	78	7	35	9	27
≥250	22	22	0	4	6	12
Σ	129	123	9	52	16	46

Tab. 63 Verteilung der Größenklassen über die Cluster

			I	II	III	IV
WZ/n	**n=129**	**n=123**	**n=9**	**n=52**	**n=16**	**n=46**
C	4	4	1	2	1	0
D	34	34	3	14	6	11
E	4	4	0	1	1	2
F	8	7	1	4	0	2
G	17	17	0	8	1	8
H	5	5	0	5	0	0
I	7	7	1	4	1	1
J	5	4	1	2	0	1
K	15	14	1	3	3	7
M	6	6	0	1	1	4
N	16	14	1	4	2	7
O	8	7	0	4	0	3
Σ	129	123	9	52	16	46
C-F	50	49	5	21	8	15
G-O	79	74	4	31	8	31

Tab. 64 Verteilung der Branchenzugehörigkeit über die Cluster

Diese Abweichungen können allerdings nicht interpretiert werden. Die Verteilung der produzierenden und dienstleistungsorientierten Unternehmen auf die vier Cluster weist keine besonderen Ausreißer auf (siehe Tab. 64). So entspricht die Besetzung der Cluster II und IV in etwa der Verteilung der Grundgesamtheit von 40% produzierenden und 60% dienstleistungsorientierten Unternehmen. In Cluster III liegt eine paritätische Besetzung vor, während in Cluster I das Verhältnis umgekehrt ist und 56% produzierende und 44% dienstleistungsorientierte Unternehmen dem Cluster zugeordnet werden.

Bei einer Betrachtung auf Ebene der Wirtschaftsabschnitte zeigt sich, dass alle vier Unternehmen aus dem Gastgewerbe (WZ-H) dem Cluster II zugeordnet sind. Zudem sind vier der sechs Unternehmen des Wirtschaftsabschnittes WZ-M Cluster IV zugeordnet. Insgesamt scheinen keine Zusammenhänge zwischen Branchenzugehörigkeit und Clusterzuweisung zu bestehen.

Im Hinblick auf die Verpflichtung zu RM sowie die Implementierung von RM- und WM-Initiativen bestehen zwischen den Clustern in der Relation zur Ausgangsverteilung folgende Besonderheiten, wobei in Tab. 65 die prozentuale Verpflichtung bzw. Implementierung abgetragen ist. Cluster I weist einen deutlich höheren Anteil an Unternehmen auf, die zum RM verpflichtet sind[319] sowie Maßnahmen in beiden Bereichen implementiert haben. Auch Cluster III weist höhere Ausprägungen in diesen drei Bereichen auf. Cluster II hingegen ist dadurch charakterisiert, dass der Anteil an Unternehmen mit implementierten RM- und WM-Initiativen geringer ist und zudem auch der Anteil an Unternehmen mit einer gesetzlichen Verpflichtung zum RM geringer ist, während die Ausprägungen in Cluster IV in etwa der Ausgangsverteilung entsprechen. Wie in Abschnitt 7.2.7 erläutert bestehen bei Unternehmen, die sowohl RM- als auch WM-Maßnahmen implementiert haben, signifikante Unterschiede im Vergleich zu Unternehmen ohne entsprechende Maßnahmen in Bezug auf die Konzepte Steuerung und Wissensqualität, wobei erstere umfassender implementiert ist und die Wissensqualität positiv abweicht. Diese Charakteristika treffen auch auf Cluster I zu, wodurch diese Aussagen nochmals gestützt werden.

			I	II	III	IV
RM/ WM /n	**n=129**	**n=123**	**n=9**	**n=52**	**n=16**	**n=46**
RM-Verpf.	0,26	0,24	0,44	0,15	0,31	0,26
RM-Ini.	0,53	0,51	0,67	0,42	0,63	0,54
WM-Ini.	0,40	0,41	0,67	0,31	0,50	0,41

Tab. 65 Verteilung der RM/WM Initiativen über die Cluster

Im Rahmen der vertiefenden empirischen Studie soll identifiziert werden auf welche Einflussfaktoren oder Steuerungsmaßnahmen spezifische Konstellationen zurückzuführen sind, um weitere Erkenntnisse zu gewinnen. Dabei können z.B. branchenspezifische oder wettbewerbsspezifische Einflussfaktoren die Relevanz bestimmter Risiken erhöhen oder reduzieren. Andererseits könnten auch weitere Steuerungsmaßnahmen in den betroffenen Unternehmen eingesetzt werden und die Ursache für die resultierende Konstellation sein. Basierend auf den Charakteristika der vier Cluster werden in nachfolgendem Abschnitt 7.4.2.3 Fragestellungen abgeleitet, die im Rahmen der vertiefenden Studie detailliert analysiert werden sollen. Dabei sind für diese Fragestellungen insbesondere die Extremwerte der einzelnen Faktoren von Relevanz, da sie auf spezifische Einflussfaktoren oder andere Steuerungsmaßnahmen schließen lassen, die identifiziert werden sollen.

[319] So sind in Cluster I 44% der Unternehmen zum RM gesetzlich verpflichtet, während der Anteil über alle Unternehmen bei 24% liegt.

Nachdem die vertiefenden Fragestellungen zur vertieften Analyse der extremen Ausprägungen der Faktoren dargelegt wurden erfolgt mittels Abb. 40 nochmals eine graphische Darstellung der Profile der Cluster. Zur besseren Visualisierung und Interpretation der Abbildung wurden die Vorzeichen bei den vier Faktoren der beiden negativen Konzepte Wissensdiffusion und Wissensverlust umgekehrt. Somit ist die Abbildung im Hinblick auf die vier beeinflussten Konzepte so zu interpretieren, dass ein negativer Wert einer vergleichsweise höheren Risikoeinschätzung bzw. einem geringeren Erfolg des Wissenstransfers oder Wissensqualitätsniveau entspricht. Analoges gilt für die positiven Werte.

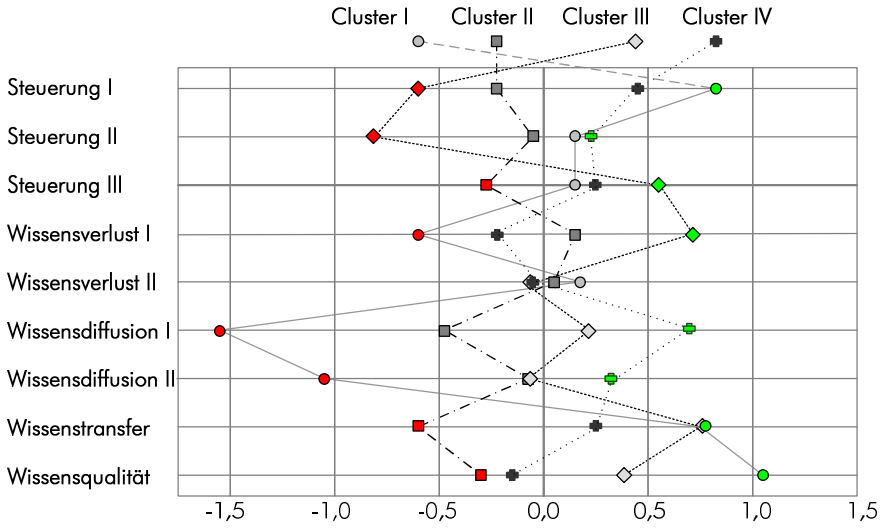


Abb. 40 Profil der Cluster

Im Hinblick auf die drei Faktoren zur Steuerung sind negative Ausprägungen als eine vergleichsweise geringere und positive Ausprägungen als vergleichsweise stärkere Steuerung zu interpretieren. Entsprechend dieser Einordnung sind die jeweiligen negativen und positiven Extremwerte abgetragen und bilden auch zugleich den Hauptuntersuchungsgegenstand der vier Cluster.

Betrachtet man die Extremwerte der Faktorausprägungen über die vier Cluster hinweg (siehe Tab. 62 und Abb. 40) so ergeben sich für die vertiefende unternehmensübergreifende Studie folgende Fragestellungen. Aufgrund der zu geringen Abweichung zwischen den Extremwerten wird der Faktor Wissensverlust II „Nichtdokumentation“ von der Betrachtung ausgeschlossen. In Tab. 66 sind die clusterspezifischen Fragestellungen der vertiefenden unternehmensübergreifenden Studie zusammengefasst.

Cluster I	1. Aus welchen Gründen begrenzen Sie vergleichsweise stark den Zugang? 2. Auf welche Einflussfaktoren ist der vergleichsweise hohe fluktuationsbedingte Wissensverlust zurückzuführen? 3. Auf welche Einflussfaktoren ist die vergleichsweise hohe wettbewerbsbedingte Diffusion zurückzuführen? 4. Auf welche Einflussfaktoren ist die vergleichsweise hohe zusammenarbeitsbedingte Diffusion zurückzuführen? 5. Auf welche Einflussfaktoren ist der vergleichsweise hohe Wissenstransfererfolg zurückzuführen? 6. Auf welche Einflussfaktoren ist das vergleichsweise hohe Niveau der Wissensqualität zurückzuführen?
Cluster II	1. Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur IT-Sicherheit? 2. Auf welche Einflussfaktoren ist der vergleichsweise niedrige Wissenstransfererfolg zurückzuführen? 3. Auf welche Einflussfaktoren ist das vergleichsweise geringere Niveau der Wissensqualität zurückzuführen?
Cluster III	1. Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur Begrenzung des Zugangs? 2. Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur Kontrolle der Weitergabe? 3. Aus welchen Gründen ergreifen Sie vergleichsweise mehr Maßnahmen zur IT-Sicherheit und welche Auswirkungen hat dies Ihrer Ansicht nach? 4. Auf welche Einflussfaktoren ist der vergleichsweise geringe fluktuationsbedingte Wissensverlust zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind?
Cluster IV	1. Aus welchen Gründen ergreifen Sie vergleichsweise mehr Maßnahmen zur Begrenzung des Zugangs? 2. Auf welche Einflussfaktoren ist die vergleichsweise geringere zusammenarbeitsbedingte Diffusion zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind? 3. Auf welche Einflussfaktoren ist die vergleichsweise geringere wettbewerbsbedingte Diffusion zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind? 4. Ist die geringere wettbewerbsbedingte Diffusion auf eine vergleichsweise stärkere Kontrolle der Weitergabe zurückzuführen?

Tab. 66 clusterspezifische Fragestellungen

Diese Fragestellungen werden im Rahmen der unternehmensübergreifenden Studie in nachfolgendem Abschnitt erörtert.

7.5 Analyse unternehmensübergreifender Besonderheiten

7.5.1 Untersuchungsgegenstände der vertiefenden Studie

Für die vertiefende unternehmensübergreifende Studie werden zwei Auswahlkriterien und Untersuchungsgegenstände herangezogen. Zum einen werden je Cluster zwei Unternehmen, die die Charakteristika des Clusters besonders gut repräsentiert, zur Analyse clusterspezifischer Fragestellungen erneut kontaktiert. Die Auswahl erfolgt dabei, wie in Abschnitt 7.4.2.3 dargstellt, in Abhängigkeit der minimalen betragsmäßigen Abweichung zu den Mittelwerten des Clusters über alle Faktoren hinweg. Hierbei bilden die aus der Analyse der Cluster abgeleiteten Fragestellungen (siehe Tab. 66) den zentralen Untersuchungsgegenstand, wobei insbesondere Extremwerte analysiert werden. Diese können u.a. auf in der Studie eingeschlossene oder weitere Steuerungsmaßnahmen sowie auf potentielle branchen- oder unternehmensspezifische Umfeldfaktoren zurückgeführt werden. Als zweite Gruppe werden diejenigen Unternehmen näher betrachtet, die in Bezug auf die Variablen der vier abhängigen Konzepte die positivsten Ausprägungen aufweisen. Dies bedeutet, dass diese Unternehmen in Bezug auf die beiden positiv operationalisierten Konzepte Wissenstransfer und Wissensqualität möglichst gering vom Maximalwert über alle 129 Unternehmen hinweg abweichen, wobei dies mit einem hohen Wissenstransfererfolg bzw. einem hohen Niveau der Wissensqualität bzw. mit einer niedrigen Ausprägung der korrespondierenden Wissensrisiken gleichzusetzen ist. In Bezug auf die beiden negativ operationalisierten Konzepte sind die Ausprägung dann positiv, wenn sie möglichst gering vom Minimum über alle 129 Unternehmen abweichen. Geringe Abweichungen vom Minimum sind demnach mit einer geringen Risikoausprägung gleichzusetzen. Summiert man diese Abweichung über alle vier abhängigen Konzepte hinweg auf, so weisen die Unternehmen mit der geringsten betragsmäßigen Abweichung die positivsten Ausprägungen auf und können im Hinblick auf den Untersuchungsgegenstand als besonders erfolgreich charakterisiert werden. Im Rahmen der vertiefenden Betrachtung von vier Unternehmen mit diesen Charakteristika, soll identifiziert werden, auf welche Einflussfaktoren bzw. Steuerungsmaßnahmen der jeweilige Erfolg zurückzuführen ist. Die spezifischen Abweichungen sind in Tab. 67, die nach den zuvor beschriebenen minimalen Abweichung über alle vier Konzept sortiert ist, zusammengefasst[320]. Dabei sind exemplarisch die fünf Unternehmen mit der geringsten Abweichung über die vier abhängigen Konzepte abgetragen. Zusätzlich umfasst die Tabelle die maximale Abweichung, die sich aus der Spannweite entsprechend der Zustimmung aller Unter-

[320] Bei dieser Art der Ermittlung der minimalen Abweichungen sei allerdings erwähnt, dass es sich hier nur um eine Näherung handelt, die zur Unterstützung der Auswahl der erfolgreichsten Unternehmen herangezogen wird, und nicht um ein statistisch korrektes Verfahren, da dies gleiche Äquidistanzen der Likert Skala voraussetzen würde und dies nicht gegeben ist.

nehmen ergibt, und den Mittelwert[321]. Aus Tab. 67 wird ersichtlich, dass je nach errechneten Abweichungen die Fragestellungen variieren. So steuert beispielsweise Unternehmen I trotz niedrigster Abweichung vom Maximum positivster Ausprägung der Konzepte vergleichsweise weniger als Unternehmen II. Zum anderen liegen bei Unternehmen III Abweichungen in Bezug auf das Konzept Wissensdiffusion über dem Durchschnitt und machen ca. 50% der Gesamtabweichung über alle Konzepte aus, wobei letztere im Vergleich zu den anderen Unternehmen gering ist. Aus diesem Grund sind die Fragestellungen von den spezifischen Charakteristika der in die vertiefende Studie einbezogenen Unternehmen abhängig und variieren. Der Grundtenor liegt aber generell auf der Erklärung der gesamthaften positiven Ausprägung und deren Zusammenhang mit der Steuerung. So können auch in diesem Fall die positiven Ausprägungen auf branchen- oder unternehmensspezifische Besonderheiten zurückzuführen sein. Eine detaillierte Erläuterung der Fragen erfolgt bei der Diskussion.

			Unternehmen				
Abweichungen	Min/Max	x	I	II	III	IV	V
gesamt	209	87	82	46	66	62	51
Steuerung von Wissensrisiken	78	36	61	23	41	35	24
Wissensverlust	34	14	8	2	3	4	3
Wissensdiffusion	34	11	4	9	12	10	9
Wissenstransfer	30	13	6	5	8	6	11
Wissensqualität	33	13	3	7	2	7	4
Abweichung Konzepte ges	131	52	21	23	25	27	27

Tab. 67 absolute Abweichungen der Konzepte

Somit werden in der vertiefenden Studie insgesamt 12 Unternehmen erneut kontaktiert, um die spezifischen Fragestellungen detailliert zu analysieren. So werden acht Unternehmen, die die vier Cluster repräsentieren, erneut telefonisch kontaktiert. Weiterhin werden mit vier Unternehmen die Ursachen der vergleichsweise positiven Ausprägungen der Konzepte fallbasiert betrachtet werden. Neben der spezifischen Analyse werden mit allen Unternehmen allgemeine Fragen erörtert. Diese zielen auf spezifische Untersuchungsgegenstände ab, die sich im Rahmen der Durchführung der Studie und in Bezug auf die Auswertung ergeben haben. Sie betreffen die Steuerung von Risiken der Wissensdiffusion, Kriterien zur Klassifikation von Wissen, Austauschbeziehungen und Ansätze zur Implementierung.

- **Steuerung der Wissensdiffusion**: Bei der Betrachtung der Steuerungsmaßnahmen in Abschnitt 7.3 hat sich gezeigt, dass die Risiken im Hinblick auf das Konzept Wissensdiffusion vergleichsweise schlecht steuerbar sind. Aus diesem Grund sollen im Rahmen der vertiefenden Studie Steuerbarkeit dieser Risiken und dabei insbesondere die Eignung weiterer Steuerungsmaßnahmen erörtert werden.
- **Klassifikation von Wissen**: Zum Zweiten hat sich in den Telefoninterviews herausgestellt, dass der Klassifikation von Wissen eine bedeutende Rolle für die Steuerung zukommt, da sie die Basis

[321] Dabei beträgt die Spannweite zumeist 6 je Variable, da sowohl eine vollkommene Zustimmung als auch eine vollkommene Ablehnung auftraten. In sieben Fällen beträgt die Spannweite allerdings 5, da die Extremkategorien nicht auftraten. Dies betrifft je zwei Variablen der Konzepte Wissensdiffusion und Wissensverlust sowie drei Variablen des Konzeptes Wissensqualität.

für weitere Steuerungsmaßnahmen, wie z.B. Geheimhaltungsvereinbarungen, Wissenstransferrichtlinien oder Kooperationsvereinbarungen, bildet. Aufgrund dieser Bedeutung sollen im Rahmen der vertiefenden Studie Kriterien bzw. Heuristiken erhoben werden, die zur Klassifikation von Wissen herangezogen werden können.

- **Austauschbeziehungen**: Bereits bei der Konzeption der Studie und auch bei der Durchführung wurde deutlich, dass Austauschbeziehungen zwischen den Konzepten bestehen. So können Steuerungsmaßnahmen einerseits Risiken reduzieren, allerdings auch andererseits positive bzw. erwünschte Prozesse hemmen. Diese Fragestellungen sollen im Rahmen der vertiefenden Studie mit allen beteiligten Unternehmen erörtert werden.
- **Implementierung der Steuerung von Wissensrisiken**: Als weiterer Analysegegenstand soll im Rahmen der vertiefenden Studie erhoben werden, wie die Steuerung von Wissensrisiken konkret in Unternehmen implementiert werden kann. Dabei spielt insbesondere die Schaffung von neuen Rollen bzw. die Übernahme von Aufgaben durch bestehende Rollen.

Eine vollständige Auflistung der für die vertiefende Studie verwendeten Fragen ist dem strukturierten Interviewleitfaden in Anhang A 2 zu entnehmen.

7.5.2 Clusterspezifische Besonderheiten

Für die vertiefende Analyse der clusterspezifischen Fragestellungen wurden je Cluster zwei Unternehmen ausgewählt und auf der Basis von Telefoninterviews die spezifischen Fragestellungen analysiert. Bei der Auswahl wurden dabei primär diejenigen Unternehmen betrachtet, die das Cluster am besten repräsentieren. Dazu wurde je Faktor die betragsmäßige Differenz ermittelt und diese Differenz ebenfalls betragsmäßig über alle Faktoren aufsummiert. Die Unternehmen mit der geringsten Abweichung über alle Faktoren hinweg repräsentieren dabei das Cluster am besten, da die Abweichungen zu den Mittelwerten am geringsten sind. In Abhängigkeit der Bereitschaft an der vertiefenden Studie teilzunehmen, wurden die Unternehmen ausgehend von einer minimalen Abweichung über alle Faktoren hinweg in aufsteigender Reihenfolge kontaktiert[322]. Die Fragestellungen für die Analyse der clusterspezifischen Besonderheiten wurden in Abschnitt 7.4.2.3 hergeleitet und sind in Anhang A 2 zusammengefasst. In Bezug auf diese Fragestellungen können je Cluster folgende Erkenntnisse gewonnen werden.

Cluster I: Die Unternehmen in Cluster I sind dadurch charakterisiert, dass sie in Bezug auf den Faktor Steuerung I „Begrenzung des Zugangs“ vergleichsweise hohe Werte aufweisen und somit in diesem Bereich stärker steuern (siehe Tab. 66, S.330, Frage I.1). Nach Angabe beider Unternehmen (Ia/ Ib)

[322] In Bezug auf Cluster I (n=9) konnten die beiden Unternehmen mit der geringsten und drittgeringsten Abweichung, für Cluster II (n=52) die mit der geringsten und fünftgeringsten, für Cluster III (n=16) die mit der geringsten und zweitgeringsten sowie für Cluster IV (n=46) die mit der geringsten und drittgeringsten Abweichung gewonnen werden.

wird der Zugang zu den Büro- bzw. Produktionsgebäuden bzw. der Zugriff auf sensitive dokumentierte Inhalte stark begrenzt. Die starke Begrenzung des Zugangs betrifft in Unternehmen Ia insbesondere die Entwicklungsabteilung, da dieser besonderer Schutz beigemessen wird. Als Gründe für die Begrenzung wurde angeführt, dass dadurch Wirtschaftsspionage durch Besucher, externe Mitarbeiter und Kooperationspartner entgegengewirkt werden soll. Im Falle von Unternehmen Ib wurde auch die hohe Fluktuation im Vertrieb angeführt, die eine Zugriffsbeschränkung auf arbeitsrelevante Inhalte zur Folge hat. Eine Hemmung interner Prozesse wird durch die Ansprechpartner nicht gesehen.

Unternehmen in Cluster I sind zudem durch eine vergleichsweise hohe Ausprägung des Faktors Wissensverlust I: „fluktuationsbedingter Wissensverlust“ charakterisiert (siehe Tab. 66, S.330, Frage I.2). Als Grund für die Interfluktuation wurde in Unternehmen Ia die im Vergleich zu den Konkurrenten geringere Unternehmensgröße von ca. 200 Mitarbeitern angeführt, die zur Folge hat, dass Mitarbeiter aus Gründen verbesserter Aufstiegschancen oder Vergütung das Unternehmen verlassen. Als weiterer Grund wurde durch den Ansprechpartner in Unternehmen Ib angeführt, dass es sich um eine Wachstumsbranche handle und diese zudem durch einen Fachkräftemangel charakterisiert ist. Dies hat zur Folge, dass Wechsel zu Konkurrenten vergleichsweise häufig auftreten und somit Nachfolgeproblematik gegeben ist. In Bezug auf die Vertretung und Reorganisation wurde durch den Ansprechpartner in Unternehmen Ib darauf hingewiesen, dass die Mitarbeiter vielfach über stark spezialisiertes Wissen verfügen und somit eine lückelose Vertretung schwer ist, zumal die Vertreter die eigenen Aufgaben zu bewältigen haben. Als weiterer Grund für fluktuationsbedingte Wissensverluste wurden in Unternehmen Ib mehrere Akquisitionen in den letzten Jahren angeführt, die zu einer Versetzung oder zum Ausscheiden der Mitarbeiter geführt haben.

Trotz einer vergleichsweise hohen Begrenzung des Zugangs sind die Unternehmen in Cluster I auch von einem vergleichsweise höheren Risiko in Bezug auf den Faktor Wissensdiffusion I „wettbewerbsbedingte Wissensdiffusion“, der Reverse Engineering, Competitive Intelligence Bestrebungen und Imitation einschließt (siehe Tab. 66, S.330, Frage I.3), betroffen. Im Falle von Unternehmen Ia ist die höhere Risikoausprägung darauf zurückzuführen, dass die Produkte relativ schwer zu schützen sind und Konkurrenten vergleichsweise leicht in der Lage sind, neue Entwicklungen zu kopieren. In Unternehmen Ib wird insbesondere der Fluktuation von Fachkräften eine besonders hohe Bedeutung für die höhere Risikoausprägung beigemessen, da diese Wissen bei Konkurrenten anwenden und so die Imitation erleichtert wird.

Neben der wettbewerbsbedingten Diffusion sind Unternehmen in Cluster I auch dadurch charakterisiert, dass im Vergleich zu den anderen Clustern eine hohe Ausprägung des Faktors Wissensdiffusion II „zusammenarbeitsbedingte Wissensdiffusion“ aufweisen, der unautorisierte Zugriffe und unerwünschten Zugang für den Partner einschließt (siehe Tab. 66, S.330, Frage I.4). Als Begründung der stärkeren Risikoausprägung wurde durch beide Ansprechpartner (Ia/ Ib) angeführt, dass die Begren-

zung primär nach außen gerichtet und bedingt durch eine offene Unternehmenskultur unautorisierte Zugriffe bzw. strikte Geheimhaltung nur schwer möglich ist. Im Falle des Unternehmens Ia bestehen auch starke persönliche Bindungen, die eine derartige Begrenzung erschweren. Weiterhin ist in Unternehmen Ib die Zusammenarbeit mit Partnern im Bereich der Entwicklung erforderlich, wobei eine Diffusion schwer zu vermeiden ist und eine zu starke Begrenzung die Zusammenarbeit hemmen würde, da so Misstrauen kommuniziert würde.

Neben zum Teil höheren Risikoausprägungen ist Cluster I auch dadurch charakterisiert, dass der Wissenstransfererfolg im Vergleich zu den anderen Clustern höher eingeschätzt wird (siehe Tab. 66, S.330, Frage I.5). In Unternehmen Ia wurde als Grund dafür die jahrelange intensive Zusammenarbeit mit Partnern, die zugleich durch starkes Vertrauen gekennzeichnet ist, angeführt. Diese ist insbesondere aufgrund der hohen Komplexität der Produkte erforderlich. Zusätzlich zu diesem Punkt wurden durch Unternehmen Ib ein enger Austausch mit der Muttergesellschaft, die starke Zusammenarbeit mit Kunden sowie starke persönliche Netzwerk angeführt.

Auch das Niveau der Wissensqualität ist in Cluster I vergleichsweise am höchsten (siehe Tab. 66, S.330, Frage I.6). Als Begründung wurde in Unternehmen Ib angeführt, dass das Unternehmen einer starken gesetzlichen Regulierung unterliegt und insbesondere Haftungsrisiken von Bedeutung sind. Aus diesem Grund ist eine hoch qualitative Dokumentation auch in Bezug auf Nachweispflichten unerlässlich und Teil der Unternehmenskultur. Im Falle von Unternehmen Ia betrifft das hohe Qualitätsniveau nicht das gesamte Unternehmen, sondern vielmehr die Entwicklungsabteilung, da in diesem Bereich entsprechende Initiativen vorangetrieben werden und eine hoch qualitative Dokumentation für eine erfolgreiche und effiziente Zusammenarbeit erforderlich ist.

Cluster II: Die Unternehmen in Cluster II weisen in Bezug auf die drei Faktoren IT-Sicherheit, Wissenstransfer und Wissensqualität Extremwerte auf, die im Rahmen der Vertiefungsinterviews näher betrachtet wurden. In Cluster II sind Maßnahmen zur IT-Sicherheit im Vergleich zu den anderen Clustern am geringsten implementiert (siehe Tab. 66, S.330, Frage II.1). Im Falle von Unternehmen IIb wurde angemerkt, dass nur vergleichsweise wenige sensitive Inhalte elektronisch dokumentiert sind und geschützt werden müssen. Aus diesem Grund werden Standardmaßnahmen ergriffen, die mehr oder minder den Maßnahmen privater Internetnutzung entsprechen und z.B. die Nutzung von Firewalls und Virenscannern sowie die Durchführung regelmäßiger Backups einschließen. Im Falle von Unternehmen IIa besteht ebenfalls eine Art Grundschutz, wobei Handlungsbedarf gesehen wird, da die IT-Systeme veraltet sind und demzufolge auch nicht mehr den aktuellen Sicherheitsanforderungen genügen. Der Handlungsbedarf ergibt sich dabei v.a. aus der zunehmenden Digitalisierung.

Die Unternehmen in Cluster II sind auch dadurch charakterisiert, dass der Faktor „Wissenstransfer“ im Vergleich zu den anderen Clustern am niedrigsten ausgeprägt ist und demzufolge der Wissenstransfererfolg vergleichsweise gering ist (siehe Tab. 66, S.330, Frage II.2). Im Falle von Unternehmen

IIb liegt der Grund dafür darin, dass Kooperationen nur eine geringe Bedeutung beigemessen wird und aus diesem Grund nur in geringem Umfang ein externer Wissenstransfer betrieben wird. Im Falle von Unternehmen IIa haben Kooperationen in der Vergangenheit nur eine untergeordnete Rolle gespielt. Bedingt durch den zunehmenden Wettbewerbsdruck und die Komplexität werden aber aktuell Kooperationen aufgebaut.

Neben dem vergleichsweise niedrigen Wissenstransfererfolg ist auch der Faktor „Wissensqualität" bei den Unternehmen dieses Clusters am geringsten ausgeprägt und folglich das Niveau der Wissensqualität vergleichsweise geringer (siehe Tab. 66, S.330, Frage II.3). Im Falle des Unternehmens IIa wurde die geringere Bewertung des Qualitätsniveaus insbesondere darauf zurückgeführt, dass die IT-Systeme relativ alt sind und somit eine schlechte Zugreifbarkeit sowie Bereitstellung der Inhalte bieten. Durch den Interviewpartner in Unternehmen IIb wurde angeführt, dass die Aufgaben im Wesentlichen standardisiert sind und zumeist nicht die Dokumentation von Wissen erfordern. Die Dokumentation ist auf den persönlichen und nicht den unternehmensweiten Bereich fokussiert.

Cluster III: Die Unternehmen in Cluster III sind im Hinblick auf Extremwerte dadurch charakterisiert, dass sie vergleichsweise weniger Maßnahmen zur Begrenzung des Zugangs und zur Kontrolle der Weitergabe ergreifen, während im Vergleich zu den anderen Unternehmen eine stärkere Implementierung von IT-Sicherheitsmaßnahmen vorliegt. Darüber hinaus zeichnet sich dieses Cluster durch eine niedrige Ausprägung des Faktors „fluktuationsbedingte Wissensverluste" aus.

Im Hinblick auf die geringere Implementierung von Maßnahmen zur Begrenzung des Zugangs (siehe Tab. 66, S.330, Frage III.1) führte der Ansprechpartner in Unternehmen IIIa an, dass unternehmensexterne Personen nur zu einem geringen Umfang im Unternehmen sind, während in Unternehmen IIIb die Zusammenarbeit mit Kunden vorwiegend an deren Standorten erfolgt.

Darüber hinaus ist in Cluster III auch der Faktor „Kontrolle der Weitergabe" im Vergleich zu den anderen Clustern niedriger ausgeprägt (siehe Tab. 66, S.330, Frage III.2). Im Falle des Unternehmens IIIa ist dies darauf zurückzuführen, dass eine Einzelstückfertigung erfolgt und somit die Aufträge eine hohe Spezifität aufweisen. Da die Produkte vollkommen an die Kundenanforderungen angepasst sind, ist eine Imitation bzw. Reverse Engineering durch Konkurrenten nicht zielführend. Darüber hinaus ist die Branche stark spezialisiert, weshalb nur wenige direkte Konkurrenten bestehen. Im Falle von Unternehmen IIIb wurden bisweilen weniger Schutzmaßnahmen ergriffen. Aufgrund von Schadensfällen wird sich dies allerdings zukünftig ändern und v.a. der Schutz durch gewerbliche Schutzrechte erhöht.

Ferner zeichnen sich Unternehmen in Cluster III dadurch aus, dass sie vergleichsweise umfassender Maßnahmen zur IT-Sicherheit ergreifen und die Mitarbeiter ein höheres Sicherheitsbewusstsein aufweisen (siehe Tab. 66, S.330, Frage III.3). Im Falle des Unternehmens IIIb ist die hohe Ausprägung der IT-Sicherheit dadurch erklärbar, dass der IT im Unternehmen eine Schlüsselrolle zukommt. Bei einem Großunternehmen mit entsprechend vielen PCs ist nach Aussage des Ansprechpartners zudem

eine hohe IT-Sicherheit von Bedeutung. Dabei wird in diesem Unternehmen zukünftig auch ein ausgefeiltes Zugriffsrechtekonzept implementiert werden. Auch in Unternehmen IIIa werden umfassende Maßnahmen zur IT-Sicherheit ergriffen, um Kundendaten und Entwicklungswissen zu schützen, wobei die hohe Spezifität des Wissens die Erfordernisse limitiert.

Als vierter Extremwert ist Cluster III durch vergleichsweise geringe fluktuationsbedingte Wissensverluste charakterisiert (siehe Tab. 66, S.330, Frage III.4). So werden diese positiven Ausprägungen in Unternehmen IIIa dadurch begründet, dass die Belegschaft vergleichsweise alt ist und somit die Wahrscheinlichkeit von Unternehmenswechseln abnimmt. Zudem bestehen relativ wenige Unternehmen, zu denen die Mitarbeiter wechseln könnten. Darüber hinaus sind die Qualifikationen der Mitarbeiter zum Teil so spezifisch, dass sie auf dem Arbeitsmarkt keinen hohen Wert haben. Aktuell sind die Nachfolgeprobleme gering, jedoch ist man sich im Unternehmen darüber bewusst, dass aufgrund des hohen Durchschnittsalters der Belegschaft zukünftig Nachfolgeplanungen erforderlich sind. Reorganisationen werden nur selten in diesem Unternehmen durchgeführt. Personalausfälle können in der Regel gut kompensiert werden, da die Mitarbeiter eng zusammenarbeiten und somit Transparenz über die Aufgaben besteht. Im Falle des Unternehmens IIIb werden die geringe Fluktuation und damit die vergleichsweise geringeren Nachfolgeprobleme mit einem guten Betriebsklima und einer relativ jungen Belegschaft begründet. Auszubildende werden in der Regel immer übernommen, um so keine Wissensverluste zu erleiden. Zudem werden Führungspositionen generell nur intern besetzt, wodurch insbesondere in diesem Bereich Kontinuität gegeben ist. Auch im Falle dieses Unternehmens werden Verluste durch Vertretung und Reorganisation gering eingeschätzt, da letztere in geringem Umfang erfolgen und Vertretungen durch andere Mitarbeiter kompensiert werden.

Cluster IV: Betrachtet man die Extremwerte über die verschiedenen Faktoren hinweg so sind in Cluster IV die drei Faktoren Kontrolle der Weitergabe sowie die beiden Faktoren zur Diffusion am höchsten ausgeprägt. Dabei ist die stärkere Implementierung der Kontrolle der Weitergabe in Unternehmen IVa dadurch zu erklären (siehe Tab. 66, S.330, Frage IV.1), dass in der Vergangenheit Schäden erlitten wurden, die zu einem Ausbau der Rechtsabteilung und zur Einführung von Genehmigungsprozessen im Hinblick auf die externe Weitergabe von Wissen führten. Im Falle des Unternehmens IVb wird Geheimhaltung fokussiert und versucht, die Loyalität der Mitarbeiter hoch zu halten.

Die vergleichsweise geringe Ausprägung des Faktors „zusammenarbeitsbedingte Diffusion“, die positiv zu interpretieren ist (siehe Tab. 66, S.330, Frage IV.2), wird in Unternehmen IVa darauf zurückgeführt, dass die Mitarbeiter im Rahmen der Zusammenarbeit mit Partnern ihren Geheimhaltungspflichten sehr gut nachkommen. Darüber hinaus ist sensitives Wissen auf wenige Schlüsselpersonen konzentriert und diffundiert somit nicht im Rahmen der Zusammenarbeit. Im Falle von Unternehmen IVb werden Zugriffsrechte nach dem „need to know“ Prinzip umgesetzt, da deren mangelnde Definition als Hauptdiffusionspunkt identifiziert wurde.

Faktor	hohe/ positivste Ausprägung	geringe/ negativste Ausprägung
Steuerung I Begrenzung des Zugangs	• (Ia/ Ib) Begrenzung des Zugangs zu sensitiven Abteilungen (i) • (Ia) Schutz vor Wirtschaftsspionage (i/e) • (Ib) hohe Fluktuation in best. Unternehmensbereichen, wie z.B. Vertrieb (i)	• (IIIa) nur wenige externe Personen im Unternehmen (i/e) • (IIIb) Zusammenarbeit bei Kunden vor Ort (i)
Steuerung II Kontrolle der Weitergabe	• (IVa) erlittene Schäden (i) • (IVb) hohe Loyalität der Mitarbeiter (i)	• (IIIa) hohe Spezifität der Produkte (Einzelstückfertigung) (i/e) • (IIIa) wenige Konkurrenten aufgrund stark spezialisierter Branche (e) • (IIIb) wenige Schäden in der Vergangenheit (i)
Steuerung III IT-Sicherheit	• (IIIb) Schlüsselrolle der IT (i) • (IIIb) Unternehmensgröße (i) • (IIIa) Schutz von Entwicklungen und Kundendaten vor unautorisierten Zugriffen (i)	• (IIa) veraltete IT-Systeme (i) • (IIb) vergleichsweise wenig sensitive elektronisch dokumentierte Inhalte (i)
Wissensverlust I fluktuationsbedingter Wissensverlust	• (IIIa) wenige Konkurrenten (e) • (IIIa) hohe Spezifität der Fähigkeiten (i) • (IIIa / IIIb) enge Zusammenarbeit zwischen Mitarbeitern kompensiert Wissensverluste (i) • (IIIa) vergleichsweise alte Belegschaft (i) • (IIIb) gutes Betriebsklima (i) • (IIIb) Übernahme von Auszubildenden (i)	• (Ia) geringe Aufstiegschancen (i) • (Ia) attraktive (größere) Konkurrenten (e) • (Ib) Wachstumsbranche und Fachkräftemangel (e) • (Ib) viele Konkurrenten (e) • (Ib) Spezialisierung des Wissens erschwert Vertretung / Nachfolge (i) • (Ib) Reorganisation aufgrund Akquisitionen (i)
Wissensdiffusion I zusammenarbeitsbedingte Wissensdiffusion	• (IVa) Definition von Geheimhaltungspflichten (i) • (IVa) Konzentration von Wissen auf Schlüsselmitarbeiter (i) • (IVb) Management der Zugriffsrechte (i)	• (Ia / Ib) Begrenzung primär nach außen (i) • (Ia / Ib) offene Unternehmenskultur (i) • (Ia) starke persönliche Bindungen (i) • (Ib) Zusammenarbeit im Bereich der Entwicklung ist mit Partnern unerlässlich (i)
Wissensdiffusion II wettbewerbsbedingte Wissensdiffusion	• (IVa) Limitation der externen Weitergabe (i) • (IVa) Positionierung in einer Nische / wenige Konkurrenten (i/e) • (IVa) geringe externe Zusammenarbeit (i/e)	• (Ia) schwer schützbare Produkte (i) • (Ia) Konkurrenten kopieren Produkte (e) • (Ib) Fluktuation von erfahrenen Mitarbeitern zu Konkurrenten (i/e)
Wissenstransfer	• (Ia) langjährige Zusammenarbeit (i/e) • (Ia) Komplexität der Produkte (i/e) • (Ia) Vertrauen (i/e) • (Ib) enger Austausch mit Muttergesellschaft (i) • (Ib) starke persönliche Beziehungen (i)	• (IIa / IIb) untergeordnete Rolle von Kooperationen[323] (i)
Wissensqualität	• (Ia) hohe Qualität der Dokumentationen ist erforderlich für Innovationen in der Entwicklungsabteilung (i) • (Ib) gesetzl. Regelungen / Haftungsrisiken (e)	• (IIa) veraltete IT-Systeme reduzieren Medienqualität (z.B. Bereitstellung, Zugreifbarkeit) (i) • (IIb) standardisierte Prozesse erfordern nur geringe Dokumentation von Wissen (i)

Tab. 68 Erklärungen für Extremwerte der Faktoren

Neben der zusammenarbeitsbedingten Diffusion ist auch die wettbewerbsbedingte Diffusion vergleichsweise gering ausgeprägt (siehe Tab. 66, S.330, Frage IV.3). Im Falle des Unternehmens IVb wird mittlerweile der gesamte Transfer nach außen stark kontrolliert, da es in der Vergangenheit Konkurrenten gelungen ist, erfolgreich Produkte des Unternehmens in relativ kurzer Zeit nachzubauen. Im Falle von Unternehmen IVa kann die geringe wettbewerbsbedingte Diffusion darauf zurückgeführt werden, dass das Unternehmen in einer Nische tätig ist und demzufolge vergleichsweise wenige Kon-

[323] Im Falle des Unternehmens IIa nimmt die Bedeutung aufgrund von zunehmender Komplexität und erhöhtem Wettbewerbsdruck zukünftig zu.

kurrenten hat. Obwohl es in der Branche verbreitet ist, sich in Verbänden zu organisieren, erfolgt dies durch das Unternehmen nicht, um eine wettbewerbsbedingte Diffusion zu unterbinden.
Für die besonders positiven bzw. negativen Ausprägungen über die Cluster hinweg lassen sich folgende Einflussfaktoren identifizieren, die in Tab. 68 zusammengefasst sind. In Tab. 68 ist zudem abgetragen, ob es sich bei den Erklärungen für die Extremwerte um unternehmensinterne (i) oder -externe (e) Faktoren handelt. Dabei ist die überwiegende Anzahl der Einflussfaktoren erstgenannter Natur und geht somit im Speziellen auf Handlungen bzw. Besonderheiten des Unternehmens zurück. Unternehmensexterne Faktoren betreffen vorwiegend die Anzahl an Konkurrenten, die Art der Brache oder die Nachfrage auf Märkten. Diese Einflussfaktoren werden zudem bei der Entwicklung von Handlungsempfehlungen in Abschnitt 8.2.4 nochmals aufgegriffen.

7.5.3 Charakteristika erfolgreicher Unternehmen

Die Ermittlung der Gründe für die positiven Abweichungen stellt den zweiten Untersuchungsgegenstand der vertiefenden unternehmensübergreifenden Studie dar. Neben der qualitativen Betrachtung von vier besonders erfolgreichen Unternehmen mittels Telefoninterviews werden nachfolgend zunächst Einflussfaktoren durch die quantitative Betrachtung der Stichprobenmerkmale der 30 Unternehmen mit den positivsten Ausprägungen abgeleitet. Als Vergleichsmaßstab werden die 30 Unternehmen herangezogen, die in Bezug auf die Wissensrisiken die schlechtesten Werte aufweisen. Nachfolgend werden für diese Teilstichproben Unternehmensgröße, Branchenzugehörigkeit, Implementierung von WM- und RM-Initiativen sowie die Steuerungsintensität als Analysegegenstände herangezogen.

- **Unternehmensgröße**: Betrachtet man den Einfluss der Unternehmensgröße in Bezug auf den Erfolg der Steuerung so zeigt sich, dass unter den Top 30 Unternehmen überproportional viele Großunternehmen[324] sind, während unter den 30 Unternehmen, die vergleichsweise weniger erfolgreich sind, nur ein geringer Anteil an Großunternehmen zu verzeichnen ist. Diese Zusammensetzung spricht dafür, dass Großunternehmen erfolgreicher mit Wissen und Wissensrisiken umgehen.
- **Branchenzugehörigkeit**: Zieht man die Branchenzugehörigkeit heran, so entsprechen auf einer grob granularen Betrachtung der Branchen in produzierenden und dienstleistungsorientierte Unternehmen die Anteile der Teilstichprobe in etwa der Gesamtstichprobe. So sind unter den Top 30 Unternehmen 40% produzierende und 60% dienstleistungsorientierte Unternehmen enthalten, während in Bezug auf die Gesamtstichprobe die Anteile bei 39% und 61% liegen. Betrachtet man alternativ die Teilstichprobe der Unternehmen mit den schlechtesten Ausprägungen so zeigt sich,

[324] Insgesamt sind 22 Großunternehmen in der Studie eingeschlossen. Dabei sind unter den Top 30 neun dieser Unternehmen, während unter den 30 Unternehmen mit dem geringsten Erfolg zwei Großunternehmen sind.

dass 60% der Unternehmen dem produzierenden Gewerbe angehören. Somit kann vorsichtig interpretiert werden, dass dienstleistungsorientierte Unternehmen in Bezug auf die vier abhängigen Konzepte erfolgreicher sind.

- **gesetzliche Verpflichtung zum RM**: Eine aggregierte Betrachtung der Korrelation zwischen den fünf Konzepten und der Variable gesetzliche Verpflichtung zum RM führt bei einem adjustierten Signifikanzniveau von $\alpha^*=0,02$[325] nach Spearman zu folgendem signifikanten Unterschied. So weisen Unternehmen mit einer gesetzlichen Verpflichtung zum RM eine signifikant höhere Wissensqualität auf (Spearmans Rho: 0,37; Signifikanz: 0,00002). Betrachtet man den Anteil der gesetzlichen Verpflichtung zum RM, so führen 50% der Top 30 Unternehmen eine derartige Verpflichtung an, während über alle 129 Unternehmen hinweg der Anteil der gesetzlichen Verpflichtung bei 26,36% liegt. Zieht man alternativ die Stichprobe, die die weniger erfolgreichen Unternehmen einschließt, heran, so geben diese Unternehmen nur in 10,00% an, dass eine derartige Verpflichtung besteht. Somit kann gefolgert werden, dass eine gesetzliche Verpflichtung zum RM positiven Einfluss auf die Wissensqualität nimmt. Auf der Basis qualitativer Aussagen kann dieser Einfluss auf erhöhte Dokumentationspflichten zurückgeführt werden.
- **Implementierung von RM-Initiativen**: Betrachtet man analog zur gesetzlichen Verpflichtung zum RM die Korrelation der Implementierung von RM-Initiativen und den fünf Konzepten bei einem adjustierten Signifikanzniveau von $\alpha^*=0,02$ nach Spearman, so ergeben sich folgende signifikante Unterschiede. So steuern Unternehmen, die RM-Initiativen implementiert haben, signifikant umfassender (Spearmans Rho: 0,35; Signifikanz: 0,00005). Weiterhin weisen diese Unternehmen eine höhere Wissensqualität (Spearmans Rho: 0,30; Signifikanz: 0,0005) sowie einen erfolgreicheren Wissenstransfer (Spearmans Rho: 0,28; Signifikanz: 0,001) auf. Darüber hinaus werden von diesen Unternehmen Wissenverluste signifikant geringer (Spearmans Rho: -0,28; Signifikanz: 0,001) eingeschätzt. Im Hinblick auf die Implementierung von RM-Initiativen hebt sich die Teilstichprobe der Top 30 Unternehmen ebenfalls ab. So ergreifen in dieser Stichprobe 66,67% der Unternehmen RM-Maßnahmen, während in Bezug auf alle 129 Unternehmen nur ein Anteil von 52,71% der Unternehmen derartige Initiativen implementiert hat. Die Unternehmen, die die schlechtesten Ausprägungen in Bezug auf die vier Konzepte aufweisen, haben RM-Initiativen mit 40,00% unterdurchschnittlich implementiert. Somit ist auch in diesem Fall davon auszugehen, dass derartige Initiativen einen positiven Einfluss auf die Konzepte Wissensqualität, Wissenstransfer und Wissensverlust nehmen. Weiterhin ergreifen diese Unternehmen umfassendere Steuerungsmaßnahmen. Diese Einflüsse können so interpretiert werden, dass Unternehmen, die

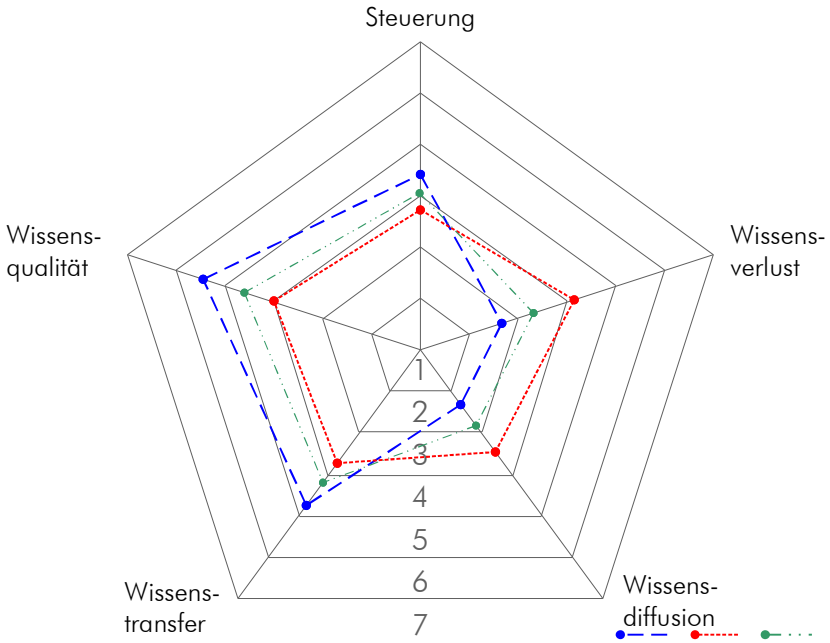
[325] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0,1/5=0,02$.

RM-Initiativen implementiert haben, umfassendere Steuerungsmaßnahmen ergreifen und ein vergleichsweise höheres Risikobewusstsein aufweisen.

- **Implementierung von WM-Initiativen:** Analog zu den beiden zuvor betrachteten Variablen ergeben sich bei einem adjustierten Signifikanzniveau von $\alpha^*=0,02$ nach Spearman signifikante Korrelationen zwischen der Implementierung von WM-Initiativen und den fünf Konzepten. So weisen Unternehmen, die WM-Initiativen implementiert haben, eine signifikant höhere Wissensqualität (Spearmans Rho: 0,34; Signifikanz: 0,00007), einen erfolgreicheren Wissenstransfer (Spearmans Rho: 0,29; Signifikanz: 0,0008) sowie geringere Wissensverluste (Spearmans Rho: -0,18; Signifikanz: 0,04) auf. Zudem ergreifen diese Unternehmen vergleichsweise umfassendere Steuerungsmaßnahmen (Spearmans Rho: 0,31; Signifikanz: 0,0003). Im Vergleich zu den RM-Initiativen wird in Bezug auf die Implementierung von WM-Initiativen der Unterschied zwischen den Top 30 und der Gesamtstichprobe noch deutlicher. So setzen von den Top 30 Unternehmen 63,33% WM-Maßnahmen ein, während der Anteil in Bezug auf die Gesamtstichprobe bei 40,31% liegt. Zieht man die Teilstichprobe mit den 30 Unternehmen mit den schlechtesten Ausprägungen heran, so zeigt sich, dass derartige Maßnahmen mit 33,33% unterdurchschnittlich implementiert sind. Demnach können die positiven Abweichungen der Unternehmen, die WM-Initiativen implementiert haben, im Vergleich zu Unternehmen ohne diese Maßnahmen in Bezug auf die Konzepte Wissensqualität, Wissenstransfer und Wissensverlust auf die Implementierung von WM-Initiativen zurückgeführt werden. Diese Einflüsse können so interpretiert werden, dass Unternehmen, die WM-Initiativen implementiert haben, ein vergleichsweise höheres Bewusstsein für den Wert des Wissens aufweisen und die Initiativen auf eine hohe Qualität sowie die Verbreitung des Wissens ausgerichtet sind.
- **Steuerungsintensität**: Zieht man zum Vergleich der Stichproben die unterschiedliche Implementierung der Steuerungsmaßnahmen heran, so zeigt sich, dass die Top 30 Unternehmen in sieben Fällen Steuerungsmaßnahmen umfassender, in vier Fällen in geringerem Maße und in zwei Fällen in etwa in gleichem Umfang implementieren. Aggregiert betrachtet steuern die Top 30 Unternehmen über alle Maßnahmen hinweg stärker, was sich in einem Mittelwert von 4,41 im Vergleich zu 3,86 im Falle der Unternehmen, die vergleichsweise weniger erfolgreich sind, niederschlägt. Diese Abweichung ist bei einem adjustierten Signifikanzniveau von $\alpha^*=0,02$ signifikant. In Bezug auf die einzelnen Steuerungsmaßnahmen besteht bei einem adjustierten Signifikanzniveau von $\alpha^*=0,0007$[326] eine signifikante Abweichung in Bezug auf die Maßnahme Redundanzschaffung, die in den Top 30 Unternehmen umfassender implementiert ist, was sich in einem Mittelwert von 4,63 niederschlägt. Dieser Mittelwert weicht von den Unternehmen, die vergleichsweise weniger

[326] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0,1/13=0,0007$.

erfolgreich sind um 1,23 positiv ab. Betrachtet man die Mittelwerte der fünf Konzepte über diese beiden Teilstichproben aggregiert, so ergeben sich in Bezug auf die fünf Konzepte deutliche Abweichungen, die in Abb. 41 dargestellt und zur Gesamtstichprobe in Bezug gesetzt sind. Dabei sind die Abweichungen über alle fünf Konzepte bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}02$ signifikant.



	erfolgreiche UN (n=30)	n. erfolgreiche UN (n=30)	gesamt (n=129)
Steuerung *	4,41	3,87	4,26
Wissensverlust *	2,69	4,07	3,39
Wissensdiffusion *	2,30	3,56	2,91
Wissenstransfer *	4,83	3,91	4,39
Wissensqualität *	5,50	4,01	4,85

Abb. 41 Ausprägungen erfolgreicher und nicht erfolgreicher Unternehmen

Demnach weisen die Top 30 Unternehmen in Bezug auf die vier abhängigen Konzepte Wissensverlust, Wissensdiffusion, Wissenstransfer und Wissensqualität geringere Risikoausprägungen auf. Zugleich haben diese Unternehmen auch signifikant umfassendere Steuerungsmaßnahmen implementiert. Ausgehend von dieser Abweichung zwischen den beiden Teilstichproben wurden im Rahmen der vertiefenden unternehmensübergreifenden Studie vier Unternehmen, die besonders positive Abweichungen aufweisen, erneut telefonisch befragt (siehe Tab. 69). In Bezug auf die in Tab. 67 dargestellten absoluten Abweichungen wurden die drei Unternehmen mit der geringsten Abweichung (Unternehmen A-C) über die vier Konzepte und das Unternehmen mit der sechstgeringsten Abweichungen (Unternehmen D) für ein Vertiefungsinterview gewonnen. Hinsichtlich Unternehmensgröße sind Unternehmen A in die Kategorie Großunternehmen, B und C als mittelständische und Unternehmen D als Kleinstunternehmen einzuordnen. Weiterhin zeigen sich auch Unterschiede in Bezug auf die Steuerungsintensität. So steuert Unternehmen A vergleichsweise stark, was sich an der Abweichung von 61 zeigt, die nah am Maximum von 78 und weit über dem Mittelwert von 36 liegt. Unternehmen C steuert in etwa dem Durchschnitt entsprechend, während die Unternehmen B und D geringer steuern.

Nachfolgend wird erörtert auf welche Einflussfaktoren bzw. Besonderheiten die vier Unternehmen die positiven Ausprägungen über die vier abhängigen Konzepte hinweg zurückführen sind.

- **Wissensverlust**: Bezogen auf die in Tab. 69 abgetragenen Mittelwerte sind alle vier vertiefend betrachteten Unternehmen geringer als der Durchschnitt von Wissensverlusten betroffen. Als Begründung führten die Unternehmen A, B und D eine hohe Belegungsstabilität und dementsprechend eine geringe Fluktuation an. Diese Stabilität ist nach Aussage der Ansprechpartner auf eine großzügige Vergabe von Weiterbildungen (A) oder vergleichsweise hohe Freiräume (C) zurückzuführen. Weiterhin werden Wissensverluste durch die Übernahme von Auszubildenden reduziert (A). Darüber hinaus tragen auch Dokumentationspflichten zu dieser niedrigen Ausprägung bei (B, C). Nach Aussage eines Ansprechpartners stellt die Dokumentation und Weitergabe des Wissens an Kollegen einen gelebten Wert im Unternehmen dar (C). Als weitere Begründung wurde eine detaillierte Nachfolgeplanung im Unternehmen angeführt (B).

			Unternehmen			
Abweichungen	Min/Max	x	A	B	C	D
gesamt	209	87	82	46	66	49
Steuerung von Wissensrisiken	78	36	61	23	41	22
Wissensverlust	34	14	8	2	3	11
Wissensdiffusion	34	11	4	9	12	0
Wissenstransfer	30	13	6	5	8	9
Wissensqualität	33	13	3	7	2	7
Abweichung Konzepte gesamt	131	52	21	23	25	27

Tab. 69 Abweichungen der ausgewählten Unternehmen

- **Wissensdiffusion:** Betrachtet man die Mittelwerte in Tab. 69 so liegen drei der vier Unternehmen in Bezug auf die Ausprägung der Wissensrisiken der Wissensdiffusion unter dem Durchschnitt, während Unternehmen C mit einem Wert von 12 knapp über dem Durchschnitt liegt. Zudem ist Unternehmen D nicht von Risiken der Wissensdiffusion betroffen, da in Bezug auf alle sechs Risiken eine minimale Risikoeinschätzung vorgenommen wurde. Der Ansprechpartner dieses Unternehmens (D) führt die geringe Risikoausprägung in diesem Bereich auf die hohe Spezifität des Wissens, den effizienten Einsatz von Geheimhaltungsvereinbarungen und die vergleichsweise gute Kontrollierbarkeit der Wissensflüsse, die sich aus der geringen Mitarbeiterzahl ergibt, zurück. Der Ansprechpartner in Unternehmen A begründete die geringe Risikoausprägung damit, dass nahezu kein Wettbewerb mit anderen Unternehmen besteht, sondern vielmehr eine kooperative Zusammenarbeit erfolgt. So werden zwischen den Unternehmen Mitarbeiter ausgetauscht und ein gemeinsames Schulungszentrum betrieben. Durch den Ansprechpartner in Unternehmen B wurde die geringe Risikoausprägung damit begründet, dass entsprechend der Anweisungen der Geschäftsleitung die externen Wissensflüsse kontrolliert werden und klar ist, welches Wissen nach außen gegeben werden darf. In Unternehmen C wurde die niedrige Risikoausprägung darauf zurückgeführt, dass sich die Mitarbeiter zum einen gegenseitig kontrollieren und zum anderen eine Weitergabe an Konkurrenten seitens der Mitarbeiter mit Reputationsverlusten für diese Mitarbeiter in der Branche einhergehen würden und dies eine erhebliche Barriere darstellt. Weiterhin ist

dokumentiertes Wissen in diesem Unternehmen durch eine hohe IT-Sicherheit vor externem unautorisierten Zugriff vergleichsweise gut geschützt.

- **Wissenstransfer**: Bezogen auf den in Tab. 69 abgetragenen Mittelwert weisen alle vier betrachteten Unternehmen überdurchschnittlich positive Ausprägungen in Bezug auf den Wissenstransfer auf. Dies wurde von allen vier Unternehmen primär dadurch begründet, dass eine intensive Zusammenarbeit mit Partnern oder Kunden erfolgt. Der Ansprechpartner in Unternehmen C führte an, dass die Partnerschaft langjährig und durch Vertrauen gekennzeichnet ist. Dennoch wird in Unternehmen D die Zusammenarbeit von vertraglichen Absicherungen flankiert, um die nachteilige Diffusion von Wissen zu vermeiden. Die Ansprechpartner in Unternehmen A und C führten an, dass die Weitergabe von Wissen einen Wert im Unternehmen darstellt, der in einem konkreten Fall (A) z.B. durch die Weiterbildung von Mitarbeitern für Mitarbeiter gelebt wird.
- **Wissensqualität**: Ebenso wie beim Konzept Wissenstransfer liegen die Ausprägungen aller vier vertieft befragter Unternehmen (siehe Tab. 69) über dem Durchschnitt und weisen somit vergleichsweise positive Werte auf. Diese positiven Ausprägungen wurden durch die Ansprechpartner der Unternehmen A und B dadurch begründet, dass sich das bestehende Qualitätsmanagementsystem positiv auf die Wissensqualität auswirkt. Weiterhin wird in den Unternehmen A und C der Dokumentation von Wissen eine hohe Bedeutung beigemessen, wobei nach Aussage des Ansprechpartners in Unternehmen A die hohe Wissensqualität in diesem Zusammenhang dadurch erklärt werden kann, dass sie eine Voraussetzung für die Nutzung der Dokumentationen darstellt. Durch den Ansprechpartner in Unternehmen C wurde weiterhin angeführt, dass der Gewährleistung der Aktualität aufgrund der kurzen Halbwertszeit von Wissen Rechnung getragen wird und eine regelmäßige Überprüfung durch themenverantwortliche Mitarbeiter erfolgt. Weiterhin führte dieser Ansprechpartner an, dass die Korrektheit von Wissen mehrfach überprüft wird, um entsprechend hochwertige Leistungen für die Kunden zu erbringen. Der Ansprechpartner in Unternehmen D führte die geringe Unternehmensgröße in Kombination mit regelmäßigen Abstimmungen, geteilten mentalen Modellen und klaren Regeln in Bezug auf die Ablage von dokumentiertem Wissen im Intranet als Gründe für eine hohe Wissensqualität an.
- **Steuerung**: Im Hinblick auf die Intensität der Steuerung liegen alle Unternehmen unter dem in Tab. 69 abgetragenen Durchschnitt. Auf die Frage hin, welchen Steuerungsmaßnahmen die größte Bedeutung zur Reduktion von Wissensrisiken beigemessen wird, trafen die Ansprechpartner folgende Aussagen. So ist in Unternehmen A die Austauschbeziehung zwischen der Verfügbarkeit und des Schutzes von sensitiven Inhalten bewusst, wobei der Verbreitung von Wissen und der Verfügbarkeit aufgrund ihrer hohen Potentiale die höchste Priorität beigemessen wird. Somit stellt die Redundanzschaffung eine wichtige Maßnahme dar. Auch in Unternehmen B wird der Verbreitung von Wissen im Sinne der Redundanzschaffung eine große Bedeutung beigemessen.

Dabei erfolgt diese Verbreitung im Kontext der Geheimhaltung. Weiterhin werden in diesem Unternehmen Maßnahmen zur Gewährleistung der Qualität des dokumentierten Wissens ergriffen, die u.a. die Sicherstellung der Korrektheit und Aktualität einschließen. Derartige Maßnahmen sind auch in Unternehmen A von hoher Relevanz, da dokumentiertes Wissen (v.a. Protokolle) vielfach von Mitarbeitern genutzt wird, die nicht an entsprechenden Sitzungen teilgenommen haben, weshalb bei der Erstellung besonders auf die Nachvollziehbarkeit geachtet wird. Der Ansprechpartner in Unternehmen C führte neben der hohen Bedeutung der Dokumentation, die v.a. die Nachbesetzung von Stellen erleichtert, an, dass die Sicherstellung von Vertrauen der Mitarbeiter sowie deren Sensibilisierung für den Schutz sensitiver Inhalte bedeutende Steuerungsmaßnahmen darstellen. Weiterhin führte der Ansprechpartner in Unternehmen C an, dass Zugriffsbeschränkungen und Sicherung der IT-Systeme primär nach außen ergriffen werden, um interne Wissensflüsse nicht zu stark zu hemmen. In Unternehmen D wurde angeführt, dass eine klare Definition der Vertraulichkeit der Inhalte und deren Implementierung in Geheimhaltsvereinbarung die bedeutendste Steuerungsmaßnahme des Unternehmens darstellt.

Konzept	Erfolgsfaktoren
Wissensverlust	• (A/B/D) hohe Belegungsstabilität (i) • (A/C) hohes akquisitorisches Potential (i/e) • (A) Übernahme von Auszubildenden (i) • (A/C) Dokumentationspflichten (i) • (B) Nachfolgeplanung (i)
	• (quant.) RM-Initiativen (i) • (quant.) WM-Initiativen (i)
Wissensdiffusion	• (A) geringe Konkurrenz / kooperativer Wettbewerb (e) • (D) hohe Spezifität des Wissens (i) • (D) geringe Mitarbeiterzahl (i) • (C) gegenseitige Kontrolle der Mitarbeiter (i) • (C) Reputationsverlust in der Branche bei Fehlverhalten (e) • (D) Einsatz von Geheimhaltungsvereinbarungen (i) • (B) Klassifikation von Wissen und Regelungen zur Weitergabe (i)
Wissenstransfer	• (A/B/C/D) enge / langjährige Zusammenarbeit mit Partnern / Kunden (i/e) • (C) Vertrauen in Partner / Kunden (i/e) • (A/C) Wissenstransfer als Wert im Unternehmen (i) • (A) Weiterbildung von Mitarbeitern für Mitarbeiter (i) • (D) vertragliche Absicherung der Zusammenarbeit (i)
	• (quant.) RM-Initiativen (i) • (quant.) WM-Initiativen (i)
Wissensqualität	• (A/B) Einsatz von Qualitätsmanagementinitiativen / -systemen (i) • (A/C) hoher Stellenwert der Dokumentation (i) • (C) laufende Aktualisierung aufgrund kurzer Halbwertszeit (i) • (C) laufende Überprüfung der Korrektheit (i) • (D) strikte Organisation der Inhalte (i)
	• (quant.) gesetzliche Verpflichtung zum RM (e) • (quant.) RM-Initiativen (i) • (quant.) WM-Initiativen (i)
Steuerung	• (A/B/C) Redundanzschaffung (i) • (C) Sicherstellung von Vertrauen und Loyalität (i) • (C) externe Zugriffsbeschränkung (i) • (B/C) Dokumentation (i) • (C) Sensibilisierung der Mitarbeiter (i) • (D) Klassifikation von Wissen (i) • (A/D) Geheimhaltungsvereinbarungen (i) • (A/B) Sicherstellung der Qualität (i)

Tab. 70 Erfolgsfaktoren der vertiefend befragten Unternehmen A-D

Die zuvor erörterten Erfolgsfaktoren bzw. Gründe für die positiven Ausprägungen der vier vertiefend befragten Unternehmen sind in Tab. 70 zusammengefasst. Dabei wird deutlich, dass die Erfolgsfaktoren primär unternehmensinterner Natur (i) sind und vergleichsweise weniger das Umfeld des Unternehmen (e), also die Wettbewerber oder Branchenspezifika, betreffen. Aus diesem Grund können diese Faktoren von Unternehmen beeinflusst werden und weisen eine gewisse Übertragbarkeit auf, weshalb sie nochmals in den Handlungsempfehlungen in Abschnitt 8.2.4 aufgegriffen werden.

7.6 Analyse unternehmensinterner Besonderheiten

7.6.1 Untersuchungsgegenstände der vertiefenden Studie

Die Analysen in den vorangegangenen Abschnitten haben gezeigt, dass im Hinblick auf die Größenklasse Unternehmen mit mehr als 250 Mitarbeitern und in Bezug auf RM- und WM-Initiativen, diejenigen Unternehmen, die Maßnahmen in beiden Bereichen einsetzen, vergleichsweise erfolgreicher mit Wissensrisiken umgehen. Entsprechend dieser Einordnung kann erwartet werden, dass ein gewisses Bewusstsein für die Thematik vorhanden ist. Aus diesem Grund wird für eine vertiefende Betrachtung ein Unternehmen herangezogen, das diese Charakteristika erfüllt. Mit diesem Unternehmen werden im Rahmen einer vertiefenden Studie unternehmensinterne Besonderheiten analysiert.

Gemäß der Kategorisierung nach den beiden Schichtungsmerkmalen (siehe Tab. 27 auf Seite 267) ist das Unternehmen als Großunternehmen im verarbeitenden Gewerbe (WZ-D) mit über 1000 Mitarbeitern einzuordnen und hat RM- und WM-Maßnahmen implementiert. Das verarbeitende Gewerbe nimmt bezogen auf alle 12 eingeschlossenen Wirtschaftsabschnitte mit insgesamt 34 Unternehmen mit 26% einen vergleichsweise großen Anteil ein. Hinsichtlich WM steht das Unternehmen am Anfang und hat aktuell Einzelinitiativen, wie z.B. den Aufbau einer Wissensdatenbank im Intranet, Dokumentation von Lessons Learned zu Projekten oder den gezielten unternehmensinternen Wissenstransfer, implementiert. Das Unternehmen plant WM-Maßnahmen zukünftig zu erweitern und dabei insbesondere auch Wissensrisiken zu berücksichtigen. Für die vertiefende Betrachtung bilden die unterschiedlichen Einschätzungen über die Geschäftsbereiche des Unternehmens hinweg den zentralen Gegenstand. Zum Zweiten soll der Einfluss der Führungsverantwortung auf die Einschätzung der Risiken analysiert werden. Daher werden sowohl Führungskräfte als auch Mitarbeiter ohne Führungsverantwortung in die Analyse einbezogen. Insgesamt wurde der Interviewleitfaden durch 66 Mitarbeiter des Unternehmens beantwortet, von denen 34 die Rolle einer Führungskraft einnehmen und 32 operative Tätigkeiten ohne Führungsverantwortung wahrnehmen.

Die Interviewpartner stammen aus den neun Geschäftsbereichen des Unternehmens. Dabei handelt es sich im Einzelnen um die in Tab. 71 dargestellten Geschäftsbereiche, die die folgenden Anteile an der Stichprobe aufweisen und als produktionsnah und kaufmännisch charakterisiert werden können. Unter

den produktionsnahen Geschäftsbereichen werden Forschung und Entwicklung, Materialwirtschaft, Produktionswirtschaft und Qualitätswesen subsumiert, während Finanz- und Rechnungswesen, Marketing, Unternehmensentwicklung, Personalwirtschaft und Betriebsrat eher kaufmännisch ausgerichtet sind. Unter Zugrundelegung dieser Schichtung erfolgte die Auswahl der Mitarbeiter innerhalb dieser neun Geschäftsbereiche durch einen Unternehmensvertreter. Entsprechend dieser Besonderheiten wurde der für die unternehmensübergreifende Studie eingesetzte Fragebogen (siehe Anhang A 1) im Hinblick auf die Abschnitte I und III angepasst. So wurden die Fragen zum Unternehmen und Person durch die Angabe des jeweiligen Geschäftsbereiches und des Status ersetzt, während durch zwei Fragen in Abschnitt III weitere Wissensrisiken und Steuerungsmaßnahmen im Kontext des Unternehmens identifiziert werden sollten. Abschnitt II, der die 37 Likert skalierten Aussagen einschließt, wurde unverändert übernommen.

Nach der Auswahl der Mitarbeiter erfolgte eine Einladung zu den Interviews. Die Interviews wurden mit jeweils zwei bis drei Mitarbeitern des Unternehmens in einem Besprechungsraum durchgeführt und durch zwei Moderatoren seitens des Unternehmens begleitet, die für das Thema sensibilisierten, den Interviewleitfaden vorstellten, die Fragen vorlasen, Fragen beantworteten und die Diskussion strukturierten. Dabei wurde den Interviewpartnern sowohl im Vorfeld als auch im Rahmen der Befragung eine anonymisierte und vertrauliche Behandlung ihrer Antworten zugesichert. Zusätzlich zur quantitativen Erhebung der Risikoeinschätzung wurden qualitative Aspekte, die sich aus der jeweiligen Diskussion ergaben, aufgenommen. Ebenso wie die Hilfskräfte auf die Kontaktierung der Unternehmen und die Durchführung der Telefoninterviews vorbereitet wurden, wurden auch die Moderatoren des Unternehmens geschult, um Durchführungsobjektivität sicherzustellen[327]. Dazu wurden die Intention der einzelnen Aussagen und deren Zusammenhänge erläutert. Diese im Rahmen der Interviews erhobenen qualitativen Aspekte ergänzen die nachfolgende Erörterung der einzelnen Konzepte.

produktionsnahe Geschäftsbereiche	
(P1) Forschung und Entwicklung	18
(P2) Materialwirtschaft	12
(P3) Produktionswirtschaft	3
(P4) Qualitätswesen	6
Σ der Teilstichprobe	39
kaufmännische Geschäftsbereiche	
(K1) Finanz- und Rechnungswesen	3
(K2) Marketing	10
(K3) Unternehmensentwicklung	9
(K4) Personalwirtschaft	2
(K5) Betriebsrat	2
Σ der Teilstichprobe	27

Tab. 71 betrachtete Geschäftsbereiche

Diesen Einschätzungen zur Steuerung von Wissensrisiken und den vier Konzepten durch die 66 Mitarbeiter aus den verschiedenen Geschäftsbereichen wird der durch die Geschäftsleitung im Rahmen der unternehmensübergreifenden Studie beantwortete Fragebogen gegenübergestellt. Dieser Fragebogen stellt gewissermaßen die aggregierte Unternehmenssicht dar und wurde im Falle dieses Unternehmens auch durch ein Gremium aus Mitgliedern der Geschäftsleitung gemeinschaftlich beantwortet. Die Abweichungen zwischen der aggregierten Unternehmenssicht und der Einschätzungen über

[327] Siehe hierzu auch Abschnitt 6.3.5.

die verschiedenen Geschäftsbereiche hinweg bilden dabei den Ausgangspunkt zur Analyse der unternehmensinternen Besonderheiten. So werden nachfolgend je Konzept potentielle Unterschiede zwischen Geschäftsbereichen sowie der Einfluss der Führungsverantwortung analysiert und dabei die Ergebnisse jeweils vor der aggregierten Unternehmenssicht gespiegelt.

7.6.2 Steuerung von Wissensrisiken

Analog zur unternehmensübergreifenden Studie werden für den unternehmensinternen Fall mittels der entsprechenden Tabellen die Verteilung der Zustimmung zu den entsprechenden Aussagen zu den einzelnen Variablen sowie die Lageparameter abgetragen. Zusätzlich werden die Tabellen um die aggregierte Sicht des Unternehmens ergänzt, wobei die jeweilige Zustimmung als separate Spalte abgetragen ist. Darüber hinaus wird die Differenz (Δa) zwischen der Unternehmenssicht und dem Median, der über alle 66 unternehmensinternen Interviews gebildet wurde, integriert, um unterschiedliche Einschätzungen zu identifizieren. Zusätzlich ist die Differenz der aggregierten Zustimmung zum Mittelwert abgetragen (Δb). Da die Unternehmenssicht keine Ausprägungen zwischen den verschiedenen Kategorien zu Zustimmung annehmen kann, wird zur Sortierung von Tab. 72 und deren Interpretation Δa herangezogen, da der Median die exakte Mitte beschreibt und in diesem Fall besser interpretierbar ist.

Tab. 72 ist aufsteigend nach der Differenz Δa und bei Gleichheit der Werte nach Δb sortiert. Eine negative Abweichung bezeichnet demnach eine geringere Einschätzung der Steuerungsmaßnahme seitens der Unternehmensleitung, während eine positive Abweichung eine höhere Einschätzung der jeweiligen Steuerungsmaßnahme bedeutet.

n=66				**Wert der Likert Skala**							**aggregierte Sicht**		
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**UN**	**Δa**	**Δb**
Redundanzschaffung	4,76	5	1,40	3	24	12	14	7	6	0	3	-2	-1,76
Zugriffsbeschränkung	5,23	6	1,37	6	31	17	1	6	5	0	4	-2	-1,23
Kooperationsvereinbarungen	2,48	2	1,68	3	2	2	11	6	17	25	1	-1	-1,48
Klassifikation von Wissen	3,33	3	2,03	4	12	6	4	8	18	14	2	-1	-1,33
IT-Sicherheitsbewusstsein	5,00	5	1,49	10	16	19	14	2	2	3	4	-1	-1,00
Dynamisierung der Zugriffsrechte	4,45	5	1,71	3	23	9	15	1	12	3	4	-1	-0,45
Zutrittsbeschränkung	2,97	2	1,91	4	7	4	6	9	19	17	2	0	-0,97
Geheimhaltungsvereinbarungen	5,05	6	1,78	10	28	10	6	1	7	4	6	0	0,95
Wissenstransferrichtlinien	3,11	2	1,80	2	6	10	9	5	20	14	3	1	-0,11
Konkurrenzschutzklauseln	4,17	4	1,79	5	12	11	22	3	3	10	5	1	0,83
Begrenzung der Interaktion	3,12	3	1,93	3	10	4	6	12	14	17	4	1	0,88
gewerbliche Schutzrechte (IP)	4,70	5	1,52	8	12	19	14	8	2	3	6	1	1,30
IT-Sicherheitsrichtlinien	3,64	4	1,82	3	11	7	15	8	12	10	5	1	1,36

Tab. 72 Verteilung, Lageparameter und aggregierte Sicht zum Konzept Steuerung

Bei Betrachtung der Tab. 72 wird ersichtlich, dass die Einschätzungen zwischen der Unternehmenssicht und den Sichtweisen der verschiedenen Geschäftsbereiche bzw. Mitarbeiter variieren, was sich

einerseits an der Standardabweichung und zum anderen an der Differenz zwischen dem unternehmensinternen Mittelwert und der Beantwortung des Fragebogens im Rahmen der unternehmensübergreifenden Studie zeigt. So wird aus Sicht der Unternehmensleitung die Implementierung der Redundanzschaffung, Zugriffsbeschränkung, Kooperationsvereinbarungen, Klassifikation von Wissen, IT-Sicherheitsbewusstsein und Dynamisierung der Zugriffsrechte im Hinblick auf Δa geringer eingeschätzt. Die Steuerungsmaßnahmen Wissenstransferrichtlinien, Konkurrenzschutzklauseln, Begrenzung der Interaktion, gewerbliche Schutzrechte und IT-Sicherheitsrichtlinien werden seitens der Unternehmensleitung als stärker implementiert angesehen, während der Median über die 66 Mitarbeiter in Bezug auf Zutrittsbeschränkungen und Geheimhaltungsvereinbarungen mit der Sicht der Unternehmensleitung korrespondiert.

Da die Steuerungsmaßnahmen hinsichtlich ihres strategischen Gehaltes variieren, ist bei zunehmend operativer Ausrichtung die Einschätzung der Mitarbeiter potentiell treffender, da deren Problemnähe vergleichsweise höher ist. Bei stärkerem strategischem Gehalt verhält es sich umgekehrt. Neben der Problemnähe wird die Einschätzung allerdings auch durch die unterschiedlichen Zielstellungen der Unternehmensleitung einerseits und der Mitarbeiter andererseits beeinflusst. So verfolgt die Unternehmensleitung in der Regel das Ziel, bestimmte Prozesse im Kontext der Steuerung eher rigide zu gestalten, während die Mitarbeiter zum Ziel haben, die Einschränkungen ihrer operativen Tätigkeiten und somit die Rigidität möglichst gering zu halten.

Neben der allgemeinen Betrachtung der Steuerungsmaßnahmen werden mittels Tab. 73 die Unterschiede zwischen produktionsnahen und kaufmännischen Geschäftsbereichen analysiert, wobei die Tabelle nach der betragsmäßigen Differenz zwischen den beiden Teilstichproben sortiert ist. Zwischen den beiden Bereichen besteht keine einheitliche Richtung der Abweichungen über das gesamte Konzept hinweg. Vielmehr werden einige Steuerungsmaßnahmen als umfassender und andere als

n=66	**Geschäftsbereiche**				n=39	n=27
Variable	**Min**	**x**	**Max**	**P**	**K**	**P-K**
Zutrittsbeschränkung	1,61	2,96	5,33	2,03	4,33	-2,31*
Geheimhaltungsvereinbarungen	2,00	5,07	6,50	5,59	4,26	1,33
Dynamisierung der Zugriffsrechte	3,17	4,46	5,67	3,92	5,22	-1,30*
Konkurrenzschutzklauseln	2,11	4,18	5,33	4,69	3,41	1,28*
Klassifikation von Wissen	1,67	3,31	6,67	2,85	4,04	-1,19
IT-Sicherheitsbewusstsein	3,50	5,03	5,67	5,31	4,56	0,75
IT-Sicherheitsrichtlinien	1,67	3,60	5,33	3,92	3,22	0,70
Kooperationsvereinbarungen	1,50	2,48	7,00	2,21	2,89	-0,68
gewerbliche Schutzrechte (IP)	2,67	4,73	5,83	4,95	4,33	0,62
Zugriffsbeschränkung	4,67	5,22	6,22	5,03	5,52	-0,49
Begrenzung der Interaktion	1,11	3,10	5,67	3,08	3,19	-0,11
Wissenstransferrichtlinien	1,78	3,16	4,33	3,13	3,07	0,05
Redundanzschaffung	3,00	4,70	5,67	4,85	4,63	0,22

Tab. 73 Steuerung im Kontext unterschiedlicher Geschäftsbereiche

weniger umfassend angesehen. Bei der Zugrundelegung von T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}0077$[328] ergeben sich folgende signifikante Abweichungen zwischen den Teilstichproben. So werden Zutrittsbeschränkungen und die Dynamisierung der Zugriffsrechte in den kaufmännischen Bereichen umfassender eingesetzt, während Konkurrenzschutzklauseln in den produktionsnahen Bereichen umfassender implementiert sind. Weiterhin wird der Zutritt zu beiden Bereichen generell durch eine Schranke mit Wachdienst und einen Empfangsbereich, an dem Besucher und Kunden abgeholt werden, kontrolliert. Die Abweichung ist dadurch erklärbar, dass die Produktionsanlagen im Vergleich zu den kaufmännischen Geschäftsbereichen vergleichsweise offen gestaltet sind, während innerhalb des kaufmännischen Bereiches die einzelnen Büros abgeschlossen sind. So ist beispielsweise in den Geschäftsbereichen Finanz- und Rechnungswesen sowie Unternehmensentwicklung, der auch die IT-Abteilung einschließt, der Zutritt zu den Büroräumen nur mit einer entsprechenden Chipkarte möglich und folglich vergleichsweise stark beschränkt. Diese Einschätzung schlägt sich auch in der vergleichsweise hohen Bewertung durch die Mitarbeiter nieder. Interessant ist dabei, dass die Zutrittsbegrenzung im Geschäftsbereich Forschung und Entwicklung am geringsten bewertet wird, wobei gerade auch in diesem Geschäftsbereich eine hohe Sensitivität gegeben ist. Die geringe Einschätzung ist darauf zurückzuführen, dass die Beschränkungen in diesem Geschäftsbereich bisweilen vernachlässigt wurden. Die Analyse dieser Fragestellungen im Rahmen der vertiefenden Studie hatte zur Folge, dass die Sicherheitsvorkehrungen in diesem Geschäftsbereich zukünftig durch den Einbau entsprechender Sicherheitstüren erhöht werden. Die Dynamisierung der Zugriffsrechte wird in den kaufmännischen Geschäftsbereichen ebenso signifikant höher eingeschätzt. Dies kann darauf zurückgeführt werden, dass elektronische Zugriffrechte in diesen Geschäftsbereichen eine vergleichsweise höhere Bedeutung aufweisen. Dies zeigt sich auch daran, dass Zugriffsrechte insgesamt vergleichsweise umfassender im kaufmännischen Bereich implementiert sind. Allerdings ist die Abweichung von 0,49 nicht signifikant. Konkurrenzschutzklauseln werden in den kaufmännischen Geschäftsbereichen signifikant geringer eingesetzt. Reflektiert man diese Abweichungen vor dem Unternehmenshintergrund, so sind die Abweichungen dadurch erklärbar, dass die Wettbewerbsvorteile und der Wertschöpfungsbeitrag in einem Unternehmen des verarbeitenden Gewerbes zu einem großen Anteil auf Innovationen zurückgeführt werden kann. Diese werden vorwiegend durch die Mitarbeiter und insbesondere Ingenieure in den produzierenden Geschäftsbereichen erbracht. Aus diesem Grund werden diese Vereinbarungen für diejenigen Mitarbeiter ergriffen, die über sensitive wettbewerbsrelevante Informationen verfügen bzw. deren Qualifikation knapp ist. So verfügen im verarbeitenden bzw. pro-

[328] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/13 = 0{,}0077$.

duzierenden Gewerbe vielfach Ingenieure über derartiges wettbewerbsrelevantes Wissen, während in dienstleistungsorientierten Branchen wiederum andere Mitarbeitergruppen betroffen sind[329].

Führungsverantwortung				
n=66		n=34	n=32	Δ
Variable	**x**	**FK**	**MA**	**FK-MA**
IT-Sicherheitsbewusstsein	5,03	5,56	4,41	1,15*
Begrenzung der Interaktion	3,10	3,56	2,66	0,90
Konkurrenzschutzklauseln	4,18	4,59	3,72	0,87
Redundanzschaffung	4,70	5,09	4,41	0,68
Dynamisierung der Zugriffsrechte	4,46	4,76	4,13	0,64
gewerbliche Schutzrechte (IP)	4,73	4,97	4,41	0,56
Kooperationsvereinbarungen	2,48	2,24	2,75	-0,51
Zugriffsbeschränkung	5,22	5,00	5,47	-0,47
Klassifikation von Wissen	3,31	3,12	3,56	-0,44
Geheimhaltungsvereinbarungen	5,07	5,15	4,94	0,21
Wissenstransferrichtlinien	3,16	3,18	3,03	0,15
IT-Sicherheitsrichtlinien	3,60	3,59	3,69	-0,10
Zutrittsbeschränkung	2,96	3,00	2,94	0,06

Tab. 74 Steuerung im Kontext der Führungsverantwortung

Mittels Tab. 74 werden die unterschiedlichen Einschätzungen der Führungskräfte und der Mitarbeiter ohne Führungsverantwortung betrachtet. Die Tabelle ist dabei ausgehend von Führungskräften nach der betragsmäßigen Differenz zwischen diesen beiden Teilstichproben sortiert. Insgesamt schätzen Führungskräfte die Implementierung bei neun der 13 Steuerungsmaßnahmen umfassender ein. Ausgehend von T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}0077$[330] wird das IT-Sicherheitsbewusstsein durch Führungskräfte signifikant höher eingeschätzt als durch operativ verantwortliche Mitarbeiter, wobei für diese Abweichung keine sachlogische Interpretation angeführt werden kann.

Neben der quantitativen Erhebung zu den einzelnen Variablen, der Errechnung der Mittelwerte und deren Vergleich über die unterschiedlichen Teilstichproben und die Unternehmenssicht hinweg, haben sich aus den Interviews zahlreiche qualitative Aspekte ergeben, die zu einem besseren Verständnis im Unternehmenskontext herangezogen werden können oder zusätzliche Aspekte beleuchten. Diese qualitativen Aspekte zu den entsprechenden Steuerungsmaßnahmen werden nachfolgend erörtert.

- **Klassifikation von Wissen**: Hinsichtlich der Klassifikation von Wissen bestehen in den verschiedenen Geschäftsbereichen Ansätze in der Form von schriftlichen Fixierungen oder mündlichen Absprachen. Allerdings besteht eine derartige Klassifikation nicht auf der aggregierten Unternehmensebene. Nach Ansicht der Interviewpartner sollte auf dieser Ebene grob festgelegt werden, welches Wissen als vertraulich gilt.
- **Zutrittsbeschränkungen**: Die Analyse der Implementierung von Zutrittsbeschränkungen über die verschiedenen Unternehmensbereiche hinweg hat ergeben, dass in einigen Geschäftsbereichen eine vergleichsweise geringere Implementierung vorliegt. Um potentielle Wissensrisiken zu ver-

[329] Als Beispiel für ein dienstleistungsorientiertes Unternehmen können Mitarbeiter mit einem umfassenden Kundenstamm angeführt werden.

[330] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/13 = 0{,}0077$.

meiden, soll die Sensibilität der Mitarbeiter für das Abschließen der Büros sowie die Beaufsichtigung von Besuchern erhöht werden. Die Interviews förderten dabei insbesondere die Austauschbeziehung zwischen Offenheit und Beschränkung zutage, der insbesondere durch eine erhöhte Sensibilität der Mitarbeiter begegnet werden kann.

- **Zugriffsbeschränkung**: Die Interviews zeigten, dass vielfache Zugriffsbeschränkungen vorhanden sind. Dies schlägt sich auch in einem vergleichsweise hohen Median von sechs nieder. Als Problem wurde in den Interviews allerdings identifiziert, dass diese Beschränkungen vergleichsweise einfach umgangen werden können, da erforderliche Rechte schnell eingeholt bzw. leichtfertig weitergegeben werden. Auch in diesem Fall wurde angeregt, dass die Balance zwischen Offenheit und Beschränkung gefunden werden muss, um nicht zu hohe Barrieren für die erwünschten Wissensprozesse zu schaffen.
- **Dynamisierung der Zugriffsrechte**: Die Interviews zeigten, dass die Dynamisierung der Zugriffsrechte eher anlassbezogen als periodisch vorgenommen wird. Somit erfolgt in der Regel keine Überprüfung der Zugriffsrechte in laufenden zeitlichen Abständen. So kommt es des Öfteren vor, dass Zugriffsrechte nicht entzogen werden und über das Dienstverhältnis hinaus bestehen bleiben.
- **Geheimhaltungsvereinbarungen**: In Bezug auf den Einsatz von Geheimhaltungsvereinbarungen wurde herausgestellt, dass derartige Vereinbarungen zwar bestehen, aber vielfach unklar ist, welches Wissen konkret der Geheimhaltung unterliegt oder nicht. Dies macht nochmals deutlich, dass der Klassifikation von Wissen eine besondere Bedeutung zukommt, da sie die Basis für eine Reihe von Steuerungsmaßnahmen bildet.
- **Wissenstransferrichtlinien**: Im konkreten Fall des untersuchten Unternehmens werden Wissenstransferrichtlinien eher in geringerem Umfang eingesetzt[331]. Das Defizit wurde erkannt und soll behoben werden, um der Diffusion von Wissen entgegenzuwirken. In einer Interviewrunde wurde vorgeschlagen, derartige Regelungen dynamisch handzuhaben und jeweils vor Projektbeginn bzw. Annahme eines Auftrags zu definieren, welches Wissen vertraulich ist und welches Wissen über die Grenzen des Unternehmens hinaus weitergegeben werden kann. Dieser Vorschlag ist insbesondere aufgrund der hohen Dynamik von Wissen besonders zu berücksichtigen.
- **Begrenzung der Interaktion**: Insgesamt wird die Begrenzung der Interaktion in diesem Unternehmen als durchschnittlich eingeschätzt. Das Erfordernis der Interaktion ist insbesondere in Geschäftsbereichen, die häufig Kontakt zu Kunden und Lieferanten haben, erforderlich. Eine Begrenzung wird eher als hinderlich erachtet.

[331] Aus Unternehmenssicht erfolgt eine Zustimmung von 3, während die Mitarbeiter die Implementierung mit einem Median von 2 bewerten.

- **Kooperationsvereinbarungen**: Im betrachteten Unternehmen werden Kooperationsvereinbarungen eher in geringem Umfang eingesetzt, wobei insbesondere die Abteilungen betroffen sind, die mit Kunden und Lieferanten im Austausch stehen. In diesen Geschäftsbereichen wurde das Problem identifiziert, dass die Inhalte der Kooperationsvereinbarungen nicht allen an den Wissenstransferprozessen beteiligten Mitarbeitern transparent sind. Somit ist auch in diesem Fall eine hohe Transparenz für die Mitarbeiter erforderlich.
- **Konkurrenzschutzklauseln**: Im konkreten Fall des vertiefend untersuchten Unternehmens werden Konkurrenzschutzklauseln immer weniger eingesetzt. Als Grund wurde angeführt, dass derartige Klauseln der Unternehmensphilosophie eines offenen Wettbewerbs widersprechen und zudem die Abwanderung qualifizierter Mitarbeiter zu Konkurrenten ein vergleichsweise geringeres Risiko darstellt[332].
- **IT-Sicherheitsrichtlinien**: Die Implementierung der Sicherheitsrichtlinien wird als mittelmäßig eingeschätzt. Die Interviews förderten allerdings zutage, dass vielfach nicht transparent ist, welche Richtlinien bestehen und wie diese im Detail ausgestaltet sind. Daran wird deutlich, dass insbesondere der Kommunikation der Richtlinien eine Bedeutung zukommt[333]. Zu diesem Zweck wurde im betrachteten Unternehmen ein Projekt in der IT-Abteilung verankert, in dessen Rahmen Sicherheitsfragestellungen aufgearbeitet werden und eine entsprechende Kommunikation an die Mitarbeiter vorgenommen wird.
- **IT-Sicherheitsbewusstsein**: Insgesamt wird in diesem Unternehmen das IT-Sicherheitsbewusstsein vergleichsweise hoch bewertet. Dabei wurde in den Interviews herausgestellt, dass das IT-Sicherheitsbewusstsein stark auf den Werten Vertrauen und Loyalität basiert und somit einen starken kulturellen Bezug aufweist. **Gewerbliche Schutzrechte**: Aufgrund der hohen Komplexität und Vielzahl der verschiedenen Patente, ist es insbesondere in Unternehmen, die dem produzierenden oder im Speziellen dem verarbeitenden Gewerbe zuzuordnen sind, zu empfehlen, spezifische Stellen bzw. Rollen zu schaffen, die sich mit der Patentanmeldung und der Verteilung relevanter Informationen befassen. Durch diese Stellen soll dabei insbesondere auch Transparenz über bestehende Patente, das Vorgehen einer Patentanmeldung sowie das Vorgehen bei einer potentielle Verletzung von Schutzrechten geschaffen werden. Dabei sind der Einsatz von gewerblichen Schutzrechten und dessen Möglichkeiten den Mitarbeitern vielfach nicht transparent und werden als komplex wahrgenommen. **Redundanzschaffung**: Zur Reduktion von Abhängigkeiten von den Schlüsselkompetenzen einzelner Mitarbeiter wird im konkreten Fall Job Rotation herangezogen.

[332] Das korrespondierende Risiko nachteilige Mitarbeiterfluktuation wurde sowohl durch die Mitarbeiter als auch durch die Unternehmensleitung mit einer 3 zugestimmt.
[333] Siehe hierzu auch Abschnitt 5.10.2.

Die zu den Steuerungsmaßnahmen gewonnenen Erkenntnisse werden nochmals in Abschnitt 7.7 aufgegriffen, und vor dem Hintergrund der Literatur reflektiert, da einige Varianten der Steuerungsmaßnahmen werthaltig sind.

7.6.3 Wissensverlust

Analog zum Konzept Steuerung von Wissensrisiken sind in Tab. 75 der Mittelwert, Median und die Standardabweichung sowie die absolute Zahl der Zustimmung zu den Aussagen abgetragen. Zudem sind die Antworten aus dem Fragebogen, der Gegenstand der breiten empirischen Studie war, aufgenommen und die Differenz aus der Sicht der Unternehmensleitung und dem Median bzw. Mittelwert über die 66 Mitarbeiter berechnet. Erstgenannte Differenz stellt zugleich das primäre Ordnungskriterium der Tab. 75 dar.

n=66				**Wert der Likert Skala**							**aggregierte Sicht**		
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**UN**	**Δa**	**Δb**
Reorganisation	3,91	4	1,77	3	12	14	10	6	16	5	2	-2	-1,91
Verlust dokumentierten Wissens	2,15	2	1,54	3	0	2	7	5	19	30	1	-1	-1,15
Nachbesetzung	3,55	3	1,96	1	18	7	2	12	14	12	3	0	-0,55
Vertretung	3,29	3	1,64	1	10	7	4	16	23	5	3	0	-0,29
Nichtdokumentation (PG)	3,15	2	1,75	2	8	9	3	8	29	7	3	1	-0,15
Nichtdokumentation (TG)	3,41	3	1,63	0	10	11	7	11	22	5	4	1	0,59

Tab. 75 Verteilung, Lageparameter und aggregierte Sicht zum Konzept Wissensverlust

Insgesamt ist bei der Beurteilung der Risiken davon auszugehen, dass diese auf der Ebene der operativen Geschäftsprozesse vergleichsweise besser eingeschätzt werden können, da die Problemnähe höher ist. Die Risikoeinschätzung weicht in vier Fällen vergleichsweise stärker ab, während sie in zwei Fällen in etwa der Sichtweise der Unternehmensleitung entspricht. Die Abweichungen, die mit einer höheren Risikoeinschätzung seitens der Mitarbeiter der verschiedenen Geschäftsbereiche einhergehen, betreffen die Risiken Reorganisation und Verlust dokumentierten Wissens. Bei dieser Abweichung kann angeregt werden, dass reorganisationsbedingte Wissensverluste durch die Mitarbeiter besser beurteilt werden können, da sie direkt davon betroffen sind, während die Unternehmensleitung nur eine aggregierte Sicht einnimmt. Ebenso ist auch davon auszugehen, dass der tatsächliche Verlust dokumentierten Wissens auf einer vergleichsweise hoch aggregierten Ebene potentiell unterschätzt wird. Auch in diesem Fall sind die Mitarbeiter stärker mit den jeweiligen Risiken konfrontiert und

n=66	**Geschäftsbereiche**			n=39	n=27	**Δ**
Variable	**Min**	**x**	**Max**	**P**	**K**	**P-K**
Nichtdokumentation (PG)	2,10	3,15	5,67	3,36	2,85	0,51*
Nachbesetzung	2,00	3,55	4,50	3,74	3,26	0,48
Reorganisation	2,17	3,91	6,00	3,77	4,11	-0,34
Vertretung	2,30	3,29	4,33	3,36	3,19	0,17
Nichtdokumentation (TG)	1,67	3,41	4,67	3,46	3,33	0,13
Verlust dokumentierten Wissens	1,67	2,15	4,00	2,13	2,19	-0,06

Tab. 76 Wissensverlust im Kontext der unterschiedlicher Geschäftsbereiche

können somit reliablere Aussagen treffen. Darüber hinaus schätzen Mitarbeiter Risiken einer Nichtdokumentation im Projektgeschäft und Tagesgeschäft vergleichsweise geringer ein.

Betrachtet man die Unterschiede zwischen produktionsnahen und kaufmännischen Geschäftsbereichen mittels Tab. 76, die nach betragsmäßigen Differenz zwischen den beiden aggregierten Unternehmensbereichen sortiert ist, so ergeben sich bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}017$[334] keinerlei signifikante Abweichungen.

Zusätzlich zur Betrachtung der Geschäftsbereiche wird mittels Tab. 77 der Einfluss der Führungsverantwortung auf die Einschätzung der Risiken im Bereich der Wissensverluste erörtert. Dabei ist die Tabelle nach der betragsmäßigen Differenz zwischen diesen beiden Teilstichproben sortiert.

Betrachtet man das Konzept gesamthaft, so schätzen Führungskräfte Risiken des Wissensverlustes geringer ein, was durch fünf negative Abweichungen deutlich wird. Unter Zugrundelegung von T-Tests bei einem analogen adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}017$ sind diese Abweichungen allerdings nicht signifikant. Beim Vergleich der Unternehmenssicht und der aggregierten Einschätzung der Wissensrisiken im Bereich Wissensverlust durch die Mitarbeiter wurde hervorgehoben, dass die Abweichungen potentiell dadurch zustande kommen, dass die Mitarbeiter aufgrund der höheren Nähe die Risiken besser einschätzen können. Im Falle der Reorganisation, die durch die Unternehmensleitung als vergleichsweise gering (Wert 2 siehe Tab. 75) eingeschätzt wird, setzt sich dieser Trend bei abnehmender Führungsverantwortung fort, da Mitarbeiter mit operativen Aufgaben die Risiken vergleichsweise höher einschätzen. Zusätzlich zu den quantitativen Erhebungen wurden in den Interviews auch qualitative Aspekte zu diesem Konzept identifiziert, die nachfolgend erörtert werden.

Führungsverantwortung				
n=66		**n=34**	**n=32**	**Δ**
Variable	**x**	**FK**	**MA**	**FK-MA**
Reorganisation	3,91	3,68	4,16	-0,48
Vertretung	3,29	3,15	3,44	-0,29
Nachbesetzung	3,55	3,41	3,69	-0,28
Nichtdokumentation (PG)	3,15	3,03	3,28	-0,25
Verlust dokumentierten Wissens	2,15	2,09	2,22	-0,13
Nichtdokumentation (TG)	3,41	3,47	3,34	0,13

Tab. 77 Wissensverlust im Kontext der Führungsverantwortung

- **Nichtdokumentation (TG / PG)**: Die Dokumentation wird insgesamt im Unternehmen gefördert und durch den Betriebsrat vorangetrieben, wobei im Projektgeschäft vergleichsweise umfassender dokumentiert wird. In den Interviews wurde allerdings auch erwähnt, dass dokumentiertes Wissen vielfach nicht ausreichend verfügbar gemacht wird. Dies zeigt auf, dass neben der Dokumentation insbesondere auch einer transparenten Verteilung des dokumentierten Wissens eine Schlüsselrolle zukommt.

[334] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/6 = 0{,}017$.

- **Nachbesetzung**: Im konkreten Fall sind Wissensverluste aufgrund einer unzureichenden Nachbesetzung eher von geringerer Relevanz, da die Nachbesetzungen vielfach langfristig bekannt sind und somit proaktive Maßnahmen zur verbesserten Einarbeitung der Nachfolger ergriffen werden können. Jedoch wurde in einigen Interviews betont, dass die Einarbeitungszeit zum Teil zu kurz ist, dadurch die Effektivität der Einarbeitung reduziert wird und somit Wissensverluste nicht vollständig vermeidbar sind.
- **Vertretung**: Im konkreten Fall wird das Risiko eines Wissensverlustes aus Vertretung vergleichsweise gering eingeschätzt, da ausreichend Transparenz der Aufgaben besteht und Wissen auch auf andere Mitarbeiter verteilt ist. Zudem leistet insbesondere auch die Dokumentation, die durch den Betriebsrat vorangetrieben wird, einen erheblichen Beitrag zur Vermeidung derartiger Verluste.
- **Reorganisation**: Im Hinblick auf Wissensverluste, die durch Reorganisation verursacht werden, wurde in den Interviews hervorgehoben, dass sich die Reorganisation bedingt durch die Vernetzungen im Unternehmen insbesondere auch auf andere Geschäftsbereiche bzw. Abteilungen auswirkt. Darüber hinaus wird die Reorganisation auch für neu rekrutierte Mitarbeiter als Problem gesehen, da sie die Einarbeitung dieser Mitarbeiter und die Etablierung von Strukturen hemmt.
- **Verlust dokumentierten Wissens**: Wissensverluste, die auf den Verlust dokumentierten Wissens zurückgehen, stellen im konkreten Fall eher die Ausnahme dar und wurden beispielsweise durch defekte Festplatten oder Wasserschäden verursacht. Als bedeutenderes Risiko wurde in diesem Kontext erwähnt, dass dokumentiertes Wissen nicht auffindbar ist, was beispielsweise auf intransparente Ablagestrukturen zurückgeführt werden kann.

Die qualitativen Erkenntnisse zeigen, dass bei der Beurteilung der Risiken des Wissensverlustes die Einschätzung der operativ verantwortlichen Mitarbeiter berücksichtigt werden sollte, auch wenn die Abweichungen auf quantitativer Ebene nicht signifikant sind.

7.6.4 Wissensdiffusion

Zur Beurteilung der Verteilung der Zustimmung zu den Aussagen sowie des Mittelwertes, Medians und der Standardabweichungen sind die entsprechenden Werte im Hinblick auf das Konzept Wissensdiffusion in Tab. 78 abgetragen. Ebenfalls ist die Differenz zwischen der Sicht der Unternehmensleitung und dem Median bzw. Mittelwert über die 66 Mitarbeiter hinweg eingeschlossen. Erstgenannte Differenz stellt zugleich das primäre Ordnungskriterium der Tabelle dar. Betrachtet man die Abweichung zwischen der Sicht der Mitarbeiter und der der Unternehmensleitung, so schätzen die Mitarbeiter drei Risiken höher ein, während die verbleibenden drei Risiken in etwa gleich eingeschätzt werden. Demnach werden die Risiken Reverse Engineering, unautorisierter Zugriffe und unerwünschter Zugang für Partner seitens der Mitarbeiter höher eingeschätzt.

n=66				Wert der Likert Skala							aggregierte Sicht		
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**UN**	**Δa**	**Δb**
Reverse Engineering	3,95	4	1,70	3	8	17	18	4	7	9	3	-1	-0,95
unautorisierte Zugriffe	2,86	3	1,31	0	1	1	29	6	15	14	2	-1	-0,86
unerwünschter Zugang für Partner	2,89	2,5	1,45	0	4	7	10	12	23	10	2	-0,5	-0,89
nachteilige Mitarbeiterfluktuation	3,68	3	2,05	4	18	4	2	15	11	12	3	0	-0,68
Competitive Intelligence	2,67	2	1,34	1	0	6	12	8	28	11	2	0	-0,67
Imitation	3,23	3	1,60	2	5	7	13	12	19	8	3	0	-0,23

Tab. 78 Verteilung, Lageparameter und aggregierte Sicht zum Konzept Wissensdiffusion

Während in Bezug auf die beiden letztgenannten Risiken diese Einschätzung durch die größere Problemnähe erklärt werden kann, stellt Reverse Engineering ein Risiko dar, das im Falle bereits realisierter Fälle aus der Perspektive der Unternehmensleitung besser beurteilt werden sollte, da deren Sichtweise aggregiert ist und somit ein gesamthafter Überblick besteht. Jedoch können die Mitarbeiter insbesondere in den produktionsnahen Geschäftsbereichen realistischer einschätzen, wie wahrscheinlich ein erfolgreiches Reverse Engineering der Produkte ist. Anhand dieses Risikos wird deutlich, dass der Einbezug verschiedener Perspektiven werthaltig sein kann.

n=66	Geschäftsbereiche			n=39	n=27	Δ
Variable	**Min**	**x**	**Max**	**P**	**K**	**P-K**
nachteilige Mitarbeiterfluktuation	2,00	3,68	4,56	3,44	4,04	-0,60
Competitive Intelligence	1,78	2,67	4,67	2,87	2,37	0,50
Reverse Engineering	3,22	3,95	6,00	3,85	4,11	-0,26
Imitation	2,50	3,23	4,67	3,15	3,33	-0,18
unautorisierte Zugriffe	2,44	2,86	4,00	2,79	2,96	-0,17
unerwünschter Zugang für Partner	2,50	2,89	4,00	2,90	2,89	0,01

Tab. 79 Wissensdiffusion im Kontext der unterschiedlicher Geschäftsbereiche

Diese unterschiedliche Betrachtung der Risiken zwischen den produktionsnahen und den kaufmännischen Geschäftsbereichen ist Gegenstand der nachfolgenden Analyse, die durch Tab. 79 gestützt wird, welche nach der betragsmäßigen Differenz zwischen den beiden aggregierten Unternehmensbereichen sortiert ist. Dabei schätzen produktionsnahe Geschäftsbereiche vier Risiken im Bereich der unerwünschten Diffusion höher ein, was durch vier negative Abweichungen deutlich wird. Legt man T-Tests bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}017$[335] zugrunde, sind diese Unterschiede zwischen den Teilstichproben allerdings nicht signifikant.

Führungsverantwortung				
n=66		**n=34**	**n=32**	**Δ**
Variable	**x**	**FK**	**MA**	**FK-MA**
unerwünschter Zugang für Partner	2,89	2,50	3,31	-0,81*
nachteilige Mitarbeiterfluktuation	3,68	3,35	4,03	-0,68
Imitation	3,23	3,32	3,13	0,20
unautorisierte Zugriffe	2,86	2,91	2,81	0,10
Competitive Intelligence	2,67	2,65	2,69	-0,04
Reverse Engineering	3,95	3,97	3,94	0,03

Tab. 80 Wissensdiffusion im Kontext der Führungsverantwortung

[335] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/6 = 0{,}017$.

Zur Analyse des Einflusses der Führungsverantwortung der Mitarbeiter sind in Tab. 80 die Mittelwerte der beiden Teilstichproben und deren Differenz abgetragen, wobei die Tabelle nach der betragsmäßigen Höhe der Differenz sortiert ist. Im Hinblick auf die Risikoeinschätzung zwischen den beiden Teilstichproben besteht bei der Betrachtung der sechs Variablen kein konsistentes Bild, da die Hälfte der Variablen seitens der Führungskräfte höher und die andere Hälfte geringer eingeschätzt wird. Bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}017$ wird nur das Risiko eines unerwünschten Zugangs für Partner signifikant niedriger durch Führungskräfte eingeschätzt. Eine Erklärung dafür könnte darin liegen, dass Mitarbeiter im operativen Tagesgeschäft mit Kooperationspartnern zusammenarbeiten und daher die daraus erwachsenden Risiken vergleichsweise stärker wahrnehmen.

Im Hinblick auf die qualitativen Erkenntnisse zu Risiken der Wissensdiffusion ergaben sich mehrere Anmerkungen aus den Interviews, die nachfolgend gesondert betrachtet werden:

- **unautorisierte Zugriffe**: Hinsichtlich des Wissensrisikos unautorisierter Zugriffe stellte sich in den Interviews heraus, dass kein breites Bewusstsein über dieses Risiko vorhanden ist und im Speziellen die IT-Abteilung eine Einschätzung vornehmen kann. So erfolgen nach Angaben der IT-Abteilung vielfach externe Versuche unautorisiert auf Wissen zuzugreifen. Diese Versuche können jedoch in der Regel erfolgreich durch entsprechende Sicherheitsmaßnahmen verhindert werden.
- **nachteilige Mitarbeiterfluktuation**: Im Rahmen der Interviews stellte sich heraus, dass ein Wechsel zu direkten Konkurrenten äußerst selten auftritt. Jedoch wurde angemerkt, dass ein solcher Wechsel bei Realisierung ein erhebliches Risiko darstellen könnte und aus diesem Grund durch die Sicherstellung der Mitarbeiterbindung durch verschiedene Maßnahmen, die das akquisitorische Potential des Unternehmens erhöhen, angestrebt werden sollte.
- **Reverse Engineering**: Die Problematik des Reverse Engineering ist im konkreten Fall abhängig von den jeweiligen Produkten. So stellt das Unternehmen Produkte für verschiedene Branchen her, die einerseits für den Massenmarkt bestimmt sind und andererseits vergleichsweise stark an die Kundenbedürfnisse angepasst sind und eine hohe Komplexität aufweisen. Insbesondere letztere sind aufgrund der hohen Komplexität und Spezifität geringer von Risiken aus Reverse Engineering betroffen, da die Destillierung des zugrunde liegenden Wissens für die Konkurrenten vergleichsweise schwerer ist. Ein großes Risiko wird in diesem Zusammenhang in Drittbeziehungen gesehen, die sich daraus ergeben, dass Konkurrenten mit den gleichen Kunden oder den gleichen Lieferanten zusammenarbeiten. So kann die Diffusion des entsprechenden Wissens über den gemeinsamen Partner erfolgen und somit das Reverse Engineering erleichtern.
- **Imitation**: Die Risiken einer Imitation gehen mit denen des Reverse Engineering einher. Auch in diesem Fall kommt den beiden Charakteristika Komplexität und Spezifität eine besondere Bedeutung zu, da sie den Erfolg der Imitation limitieren können.

- **Competitive Intelligence**: Das Risiko erfolgreicher Competitive Intelligence Bestrebungen seitens der Konkurrenz wird vergleichsweise gering eingeschätzt. Dies ist insbesondere darauf zurückzuführen, dass in der Vergangenheit eine Sensibilisierung der Mitarbeiter erfolgte und gezielte Maßnahmen zur Erschwerung ergriffen wurden. So ist der Einsatz von Kameras und Fotohandys bei der Besichtigung des Werkes untersagt. Ebenso wird versucht die unternehmensexterne Weitergabe von Wissen stärker zu kontrollieren.
- **unerwünschter Zugang für Partner**: Der unerwünschte Zugang zu Wissen für Partner wird als Risiko gesehen. Für dessen Bewältigung gelten dabei die gleichen Ansätze wie bei der externen Weitergabe von Wissen. Dieses Risiko wird nach Angaben der Kooperationsverantwortlichen zudem durch die Dauer der Beziehung und das Vertrauensverhältnis beeinflusst, wobei mit zunehmender Dauer das Vertrauensverhältnis zunimmt.

7.6.5 Wissenstransfer

Analog zu den anderen Konzepten sind in Tab. 81 Mittelwert, Median, Standardabweichung und die Verteilung der Zustimmung zu den Aussagen abgetragen, wobei die Differenz zur Unternehmenssicht ebenfalls in der Tabelle aufgeführt ist.

n=66				**Wert der Likert Skala**							**aggregierte Sicht**		
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**UN**	**Δa**	**Δb**
Erweiterung der Wissensbasis	5,41	6	0,94	3	33	23	3	3	1	0	5	-1	-0,41
Reduktion der Abhängigkeit	5,12	5	1,13	2	28	21	9	3	3	0	4	-1	-1,12
Beitrag externen Wissens	5,50	6	1,23	9	33	15	4	2	2	1	6	0	0,50
Quantität externen Wissens	5,05	5	1,16	4	23	20	11	7	1	0	5	0	-0,05
Qualität externen Wissens	5,23	5	1,02	3	27	24	7	4	1	0	6	1	0,77

Tab. 81 Verteilung, Lageparameter und aggregierte Sicht zum Konzept Wissenstransfer

Die Sortierung erfolgt primär nach der Differenz zum Median und sekundär nach der Differenz zum Mittelwert. Bezüglich der Einschätzung des Erfolgs des Wissenstransfers besteht keine einheitliche Richtung der Abweichungen. So werden die Erweiterung der Wissensbasis und die Reduktion der Abhängigkeit vom Wissen des Partners seitens der Mitarbeiter höher eingeschätzt, während die Qualität externen Wissens geringer eingeschätzt wird. Hinsichtlich der beiden anderen Variablen korrespondieren die Sichtweisen der Mitarbeiter mit denen der Unternehmensleitung.

n=66	Geschäftsbereiche			n=39	n=27	Δ
Variable	**Min**	**x**	**Max**	**P**	**K**	**P-K**
Beitrag externen Wissens	4,67	5,50	6,67	5,31	5,78	-0,47
Qualität externen Wissens	4,58	5,23	6,00	5,05	5,48	-0,43
Zunahme Unabhängigkeit	4,83	5,12	5,67	5,03	5,26	-0,23
Quantität externen Wissens	4,40	5,05	6,00	5,10	4,96	0,14
Erweiterung der Wissensbasis	4,33	5,41	6,00	5,36	5,48	-0,12

Tab. 82 Wissenstransfer im Kontext der unterschiedlicher Geschäftsbereiche

Betrachtet man die unterschiedlichen Einschätzungen des Wissenstransfererfolges über die zusammengefassten produktionsnahen und kaufmännischen Geschäftsbereiche (siehe Tab. 82), so wird ersichtlich, dass der Erfolg seitens kaufmännischer Geschäftsbereiche vergleichsweise höher eingeschätzt wird, da vier der fünf Variablen positiv abweichen. Dabei sind diese Abweichungen allerdings bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}02$ nicht signifikant[336].

Führungsverantwortung				
n=66		n=34	n=32	Δ
Variable	**x**	**FK**	**MA**	**FK-MA**
Qualität externen Wissens	5,23	5,44	5,00	0,44
Quantität externen Wissens	5,05	5,24	4,84	0,39
Zunahme Unabhängigkeit	5,12	5,24	5,00	0,24
Erweiterung der Wissensbasis	5,41	5,50	5,31	0,19
Beitrag externen Wissens	5,50	5,56	5,44	0,12

Tab. 83 Wissenstransfer im Kontext der Führungsverantwortung

Insgesamt sind die Teilstichproben vergleichsweise homogen und können folglich nicht zu einer detaillierten Diskussion herangezogen werden. Zusätzlich zur Betrachtung der Geschäftsbereiche wird nachfolgend auf Basis von Tab. 83 der Einfluss der Führungsverantwortung auf die Einschätzung des Wissenstransfererfolges erörtert, wobei die Tabelle nach der betragsmäßigen Mittelwertabweichung sortiert ist. Dabei schätzen Führungskräfte den Wissenstransfererfolg in Bezug auf alle fünf Variablen höher ein. Diese Abweichungen zwischen den Teilstichproben sind allerdings bei einem bei einem adjustierten Signifikanzniveau von $\alpha^* \leq 0{,}02$ nicht signifikant. Zudem sind die Abweichungen zwischen den Teilstichproben sehr gering, weshalb an dieser Stelle keine detaillierte Diskussion erfolgt.

Im Hinblick auf die qualitativen Erkenntnisse zu den Variablen zur Operationalisierung des Wissenstransfererfolges ergaben sich mehrere Anmerkungen aus den Interviews, die nachfolgend gesondert betrachtet werden. Im Vergleich zu den beiden negativ operationalisierten Konzepten wurde über dieses Konzept jedoch zumeist allgemein diskutiert, da sich die betrachteten Variablen in geringerem Maße unterscheiden. Daher wird das Konzept auch gesamthaft betrachtet. Insgesamt wird der Wissenstransfererfolg im Unternehmen hoch eingeschätzt, was daran deutlich wird, dass die Mittelwerte aller Variablen über fünf liegen. Weiterhin hat insbesondere auch die Dauer der Beziehung zum jeweiligen Partner einen positiven Einfluss auf den Wissenstransfererfolg, da über eine bestimmte Zeitdauer ein Vertrauensverhältnis aufgebaut werden kann. Darüber hinaus wird der Wissenstransferer-

[336] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/5 = 0{,}02$.

folg negativ durch die Komplexität des transferierten Wissens beeinflusst, da mit zunehmender Komplexität die Nachvollziehbarkeit abnimmt. Als weiterer Punkt wurde angemerkt, dass die unternehmensinterne Nutzung des transferierten Wissens zum Teil gering ist und somit noch Potentiale zur Verbesserung vorhanden sind.

7.6.6 Wissensqualität

In Tab. 84 sind Mittelwert, Median und Standardabweichung sowie die Verteilung der Zustimmung zu den Aussagen im Hinblick auf das Konzept Wissensqualität abgetragen. Dabei ist Tab. 84 primär nach der Differenz der Unternehmenssicht zum Median (Δa) und sekundär nach der Differenz zum Mittelwert (Δb) aufsteigend sortiert. Die Wissensqualität wird seitens der Mitarbeiter in vier Fällen höher bewertet, wobei zwei Variablen mit der Unternehmenssicht korrespondieren.

n=66				**Wert der Likert Skala**							**aggregierte Sicht**		
Variable	**x**	**x_{med}**	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**UN**	**Δa**	**Δb**
Nachvollziehbarkeit	5,52	6	1,26	12	30	13	4	5	2	0	4	-2	-1,52
Verfügbarkeit	5,12	5,5	1,48	12	21	12	8	10	3	0	4	-1,5	-1,12
Rechtzeitigkeit	4,95	5	1,37	5	26	13	7	13	2	0	4	-1	-0,95
Anwendbarkeit	4,52	5	1,44	2	17	20	10	9	7	1	4	-1	-0,52
Korrektheit	5,80	6	1,06	16	31	13	3	2	1	0	6	0	0,20
Aktualität	4,65	5	1,40	2	22	13	16	7	5	1	5	0	0,35

Tab. 84 Verteilung, Lageparameter und aggregierte Sicht zum Konzept Wissensqualität

Betrachtet man die Unterschiede zwischen produktionsnahen und kaufmännischen Geschäftsbereichen auf der Basis von Tab. 85, die aufsteigend nach der Mittelwertabweichung zwischen den beiden Teilstichproben sortiert ist, so wird ersichtlich, dass kaufmännische Geschäftsbereiche die Wissensqualität höher einschätzen, was sich in einer höheren Bewertung von fünf der sechs Variablen zeigt. Die Abweichungen sind jedoch bei einem Signifikanzniveau von $\alpha^* \leq 0{,}017$[337] nicht signifikant. Neben Unterschieden zwischen den Geschäftsbereichen wird auf Basis von Tab. 86 der Einfluss der Führungsverantwortung analysiert, wobei die Tabelle aufsteigend nach den betragsmäßigen Mittelwertabweichungen zwischen den korrespondierenden Teilstichproben sortiert ist. In diesem Fall ergeben sich bei analogem Signifikanzniveau keine signifikanten Abweichungen zwischen den Teilstichproben.

n=66	**Geschäftsbereiche**			n=39	n=27	**Δ**
Variable	**Min**	**x**	**Max**	**P**	**K**	**P-K**
Verfügbarkeit	3,67	5,12	6,00	4,77	5,63	-0,86
Anwendbarkeit	3,44	4,52	5,33	4,23	4,93	-0,70
Korrektheit	5,17	5,80	6,22	5,67	6,00	-0,33
Aktualität	3,33	4,65	5,67	4,56	4,78	-0,21
Rechtzeitigkeit	3,00	4,95	5,70	4,92	5,00	-0,08
Nachvollziehbarkeit	5,00	5,52	6,00	5,54	5,48	0,06

Tab. 85 Wissensqualität im Kontext der unterschiedlicher Geschäftsbereiche

[337] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^* = 0{,}1/6 = 0{,}017$.

Führungsverantwortung				
n=66		n=34	n=32	Δ
Variable	**x**	**FK**	**MA**	**FK-MA**
Anwendbarkeit	4,52	4,29	4,75	-0,46
Verfügbarkeit	5,12	4,94	5,31	-0,37
Aktualität	4,65	4,82	4,47	0,35
Rechtzeitigkeit	4,95	5,12	4,78	0,34
Korrektheit	5,80	5,68	5,94	-0,26
Nachvollziehbarkeit	5,52	5,53	5,50	0,03

Tab. 86 Wissensqualität im Kontext der Führungsverantwortung

Analog zum Wissenstransfer werden die qualitativen Aspekte zum Konzept Wissensqualität global betrachtet, da zum einen vergleichsweise weniger Anmerkungen in den Interviews gemacht wurden und zum anderen eine relativ homogene Bewertung der Variablen erfolgte.

Insgesamt wird das Niveau der Wissensqualität hoch bewertet. Im Rahmen der Interviews wurde allerdings angemerkt, dass einige Inhalte im Intranet veraltet sind. Diesem Problem wurde entgegengehalten, dass der Aktualisierungsaufwand unverhältnismäßig hoch sei. An dieser Stelle wird eine Austauschbeziehung deutlich, die es beim gezielten Umgang mit Wissensrisiken zu beachten gilt. Wie schon bei der Diskussion der Wissensverluste erwähnt, ergeben sich Wissensverluste vielfach daraus, dass dokumentiertes Wissen nicht auffindbar ist. Dies kann insbesondere darauf zurückgeführt werden, dass zum einen zahlreiche Laufwerke bestehen und zum anderen seitens der Mitarbeiter unklar ist, welche Laufwerke genutzt werden sollen. Somit ist es erforderlich, systemseitig Transparenz zu schaffen. Als Alternative wurde angeregt eine Suchmaschine einzurichten. Als weiteres Risiko wurde in den Interviews angemerkt, dass die Korrektheit des dokumentierten Wissens als sehr hoch und gegeben eingeschätzt wird. Dies zeigt sich auch an dem vergleichsweise hohen Mittelwert von 5,8 und einer vergleichsweise geringen Standardabweichung von 1,06. Das Risiko besteht demnach darin, dass sich Mitarbeiter zu stark auf dokumentiertes Wissen verlassen und keine alternativen Problemlösungen heranziehen.

7.6.7 Zusatzfragen

Nachdem die Ausprägung der einzelnen Konzepte und der entsprechenden Variablen in verschiedenen Teilstichproben erörtert wurde, werden nachfolgend zusätzlich Fragen, die nicht Gegenstand der Operationalisierung der Konzepte sind, dargelegt. Dabei handelt es sich im Einzelnen um die Bedeutung der Ressource Wissen, die Nennung weiterer Steuerungsmaßnahmen, die Priorisierung der Steuerungsmaßnahmen und die Nennung weiterer Wissensrisiken.

Bedeutung der Ressource Wissen: Die Bedeutung der Ressource Wissen wird über die 66 Mitarbeiter hinweg analog zur Unternehmenssicht hoch eingeschätzt. So schätzen 93,94% der befragten Mitarbeiter ihre Bedeutung für die Generierung der Wertschöpfung und der Wettbewerbsvorteile als hoch bzw. sehr hoch ein. Die minimale Zustimmung liegt bei einem Wert von 5. Somit ergibt sich ein Median von 7 und ein Mittelwert von 6,47. Diese Werte korrespondieren dabei auch mit der Sicht der

Unternehmensleitung, da diese ebenfalls die Bedeutung der Ressource Wissen als sehr hoch einschätzt und der Aussage mit 7 zugestimmt hat.

Bedeutung der Ressource Wissen	**n=66**				**Wert der Likert Skala**						
	UN	x	x_{med}	**σ**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
	7	6,47	7	0,61	35	27	4	0	0	0	0
	Geschäftsbereiche				**Min**	**P/K**	**Max**	**P/K**	**P**	**K**	**P-K**
					6,00	K4	7,00	K5	6,51	6,41	0,11
	Führungsverantwortung								**FK**	**MA**	**FK-MA**
									6,62	6,31	0,31

Tab. 87 Bedeutung der Ressource Wissen im unternehmensinternen Kontext

Diese hohen Einschätzungen erstrecken sich bei einer geringen Streuung über die verschiedenen Geschäftsbereiche und die unterschiedlichen Mitarbeitergruppen. Signifikante Unterschiede bestehen nicht.

Weitere Steuerungsmaßnahmen: Zusätzlich zu den Variablen zu den fünf Konzepten wurden in die vertiefende Studie drei Fragen zur Identifikation weiterer Steuerungsmaßnahmen, zu deren Priorisierung und zur Identifikation weiterer unternehmensspezifischer Wissensrisiken eingeschlossen.

Als zusätzliche Steuerungsmaßnahmen wurden dabei insbesondere Meetings, Lessons Learned, unternehmensinterne Personalentwicklung, Workshops und Aufbau einer Wissensdatenbank genannt und nachfolgend kurz erläutert:

- **Meetings / Workshops**: Eine Steuerung von Wissensrisiken kann auch dadurch erfolgen, dass im Unternehmen auf Projekt- und Abteilungsebene regelmäßig Meetings abgehalten werden. In diesem Kontext kann beispielsweise der Status des Projektes bzw. der Aufgaben erörtert, spezifische Probleme gelöst und Wissen zu bestimmten Teilaspekten ausgetauscht werden. Analog zu den Meetings wurden Workshops als Steuerungsmaßnahmen genannt. Dabei sollen Workshops dazu dienen, Mitarbeiter zur Erörterung spezifischer Fragestellungen und der Lösung von Problemen zusammenzuziehen. Im Hinblick auf die zuvor genannten Wissensrisiken eignen sich Meetings bzw. Workshops insbesondere auch dazu, Wissensverluste, die sich aus der Vertretung, Reorganisation oder Nachbesetzung ergeben, zu vermeiden oder zu vermindern, da sie einen Beitrag zur Verteilung von Wissen leisten.
- **Lessons Learned**: Im Rahmen von Projekten können gezielt Lessons Learned erarbeitet werden, die dazu dienen, Probleme, Fehler und Verbesserungspotentiale in Projekten zu reflektieren. Im konkreten Fall werden zu bestimmten Meilensteinen in Projekten Besprechungen abgehalten, um die gesammelten Erfahrungen festzuhalten, zu erörtern und für nachfolgende Projekte bzw. Problemstellungen schriftlich zu fixieren. Somit stellt diese Maßnahme eine hybride Form der zuvor genannten Meetings und der Dokumentation im Projektgeschäft dar, da die Ergebnisse dokumentiert werden und zur verbesserten Durchführung nachfolgender Projekte genutzt werden sollen.

Diese Maßnahme wirkt dabei primär der Nichtdokumentation von Wissen im Projektgeschäft entgegen, kann aber auch zur Verteilung von Wissen beitragen.

- **Personalentwicklung**: Als weitere Steuerungsmaßnahme wurde eine gezielte Personalentwicklung in der Form von Schulungen, die unternehmensintern durch die Mitarbeiter durchgeführt werden und zur Verbreitung von Wissen dienen, genannt. So werden entsprechend der Bedarfe der Mitarbeiter z.B. Schulungen zu Arbeitsrecht oder IT-Sicherheit von anderen Mitarbeitern, die in den jeweiligen Themengebieten über Expertise verfügen, durchgeführt. Im Hinblick auf die dargestellten Risiken und Steuerungsmaßnahmen korrespondiert diese Maßnahme primär mit der Redundanzschaffung, die auf die Verteilung des Wissens von Schlüsselmitarbeitern abzielt.
- **Wissensdatenbank**: Als zusätzliche Maßnahme wurde der Aufbau einer so genannten Wissensdatenbank im Intranet angeführt. Dabei handelt es sich um eine themenbasierte Ablagestruktur für dokumentiertes Wissen, die im Geschäftsbereich Forschung und Entwicklung genutzt wird. Wie bereits bei der Steuerungsmaßnahme Dokumentation und dem Konzept Wissensqualität erörtert, werden insbesondere bei der Verbreitung von Wissen Defizite erkannt. Zudem besteht im konkreten Fall dieses Unternehmens das Problem, dass aufgrund der zahlreichen vorhandenen Laufwerke einerseits Unklarheit über die Ablage dokumentierten Wissens und andererseits Defizite im Hinblick auf dessen Auffindbarkeit bestehen. Beide Risiken könnten durch eine zentrale Ablagestruktur im Intranet reduziert werden, da so ein zentraler Speicherort bestünde und somit die Freiheitsgrade bzw. Auswahlentscheidungen begrenzt würden.
- **Mitarbeiterbindung**: Auch wenn Wissensrisiken im Hinblick auf die nachteilige Mitarbeiterfluktuation in der Vergangenheit in geringem Umfang aufgetreten sind, so besteht im Unternehmen dennoch ein Bewusstsein für dieses Risiko und folglich das Ziel, proaktiv dem Eintritt einer derartig nachteiligen Abwanderung entgegenzuwirken. Als zusätzliche Maßnahme wurde daher die gezielte Bindung der Mitarbeiter durch ein akquisitorisches Potential, das in der Relation zu Konkurrenten wettbewerbsfähig ist, genannt. Dies schließt u.a. ein marktgängige Vergütung, Aufstiegschancen und ein gutes Arbeitsklima ein.

Priorisierung der Steuerungsmaßnahmen: Neben den zusätzlichen Steuerungsmaßnahmen sollten im Rahmen der Interviews auch die drei bedeutendsten Steuerungsmaßnahmen identifiziert werden. Am bedeutendsten wurden seitens der Mitarbeiter Geheimhaltungsvereinbarungen, Wissenstransferrichtlinien und Zugriffsbeschränkungen genannt. Zudem wurden die zusätzlichen Steuerungsmaßnahmen Mitarbeiterbindung und Organisation der Ablage in Form einer Wissensdatenbank angeführt, die nicht Gegenstand des Interviewleitfadens ist. Im Hinblick auf die beiden erstgenannten Maßnahmen wurde seitens der Mitarbeiter betont, dass ihnen eine besondere Bedeutung im Hinblick auf die Sicherung der Wettbewerbsvorteile zukommt. So soll durch diese Maßnahmen klar geregelt werden, welches Wissen weitergegeben werden kann oder nicht und welche Sanktionen bei einer potentiellen

Nichtbeachtung zu erwarten sind. Diesen beiden Maßnahmen erfordern allerdings eine entsprechende Klassifizierung des Wissens im Hinblick auf dessen Vertraulichkeit oder Wettbewerbsrelevanz. Auch elektronischen Zugriffsbeschränkungen auf dokumentiertes Wissen wurden als sehr relevant eingeschätzt, um den Zugriff nicht autorisierter Mitarbeiter und somit eine unerwünschte Diffusion zu verhindern. Bei dieser Steuerungsmaßnahme gilt es allerdings zu beachten, das geeignete Maß an Beschränkung und Offenheit zu finden, da durch eine zu starke Begrenzung erwünschte Prozesse gehemmt werden können.

weitere Wissensrisiken: Neben zusätzlichen Steuerungsmaßnahmen wurden im Rahmen der Interviews auch weitere Wissensrisiken im Kontext des Unternehmens erhoben. Dabei wurden folgende Wissensrisiken identifiziert:

- **unvergütete Diffusion an Kunden**: Im Zusammenhang mit der Anbahnung von Geschäften mit Kunden werden umfassende Produktdetails an die Kunden weitergegeben, obwohl kein Geschäft zustande kommt. So wird Wissen weitergegeben, ohne dass das Unternehmen eine entsprechende Gegenleistung erhält.
- **Diffusion über Drittbeziehungen**: Durch die Zusammenarbeit von Konkurrenten mit den gleichen Partnern kann Wissen indirekt über Drittbeziehungen diffundieren und daraus ein Schaden in Form des Verlustes der Wettbewerbsrelevanz auftreten.
- **mangelnde Transparenz über Regelungen**: Ein weiteres Wissensrisiko ist darin zu sehen, dass zum Teil nicht transparent ist, welches Wissen weitergegeben werden kann oder nicht, IT-Sicherheitsrichtlinien, Geheimhaltungsvereinbarungen oder auch Kooperationsvereinbarungen unzureichend bekannt sind. Aufgrund dieser Defizite ist nicht transparent, wie mit Wissen im Hinblick auf eine effiziente Steuerung umzugehen ist.
- **unzureichende strategische Personalbedarfsplanung**: Hinsichtlich des Personalmanagements besteht ein weiteres identifiziertes Risiko darin, dass der zukünftige Personalbedarf zu reaktiv geplant wird und demzufolge qualifizierte Mitarbeiter nicht ausreichend und zeitgerecht rekrutiert werden können. Dies hat zur Folge, dass bei der Durchführung der Geschäftsprozesse Mängel auftreten und geht folglich mit den kompetenzbezogenen Wissensrisiken, die dem Konzept Wissensqualität zugeordnet sind, einher.

7.6.8 Diskussion

Die Analyse der unternehmensinternen Besonderheiten der Steuerung von Wissensrisiken und der vier abhängigen Konzepte hat gezeigt, dass sich zum einen Abweichungen zur Unternehmenssicht und zum anderen zwischen den Teilstichproben ergeben. Dabei betreffen die Abweichungen ausschließlich das Konzept Steuerung, während die vier abhängigen Konzepte über die verschiedenen Teilstichproben vergleichsweise homogen eingeschätzt werden.

Die unterschiedlichen Einschätzungen können dabei darauf zurückgeführt werden, dass einerseits die Problemnähe über die Mitarbeitergruppen hin zur Unternehmensleitung variiert und zum anderen unterschiedliche Zielsetzungen bestehen. Insgesamt ist der Einbezug von Mitarbeitern unterschiedlicher Geschäftsbereiche und Hierarchiestufen in die Analyse der Steuerung von Wissensrisiken werthaltig, da bedingt durch die operative Ausrichtung auf die Ebene der Geschäftsprozesse insbesondere auch Mitarbeiter, die im Tagesgeschäft Aufgaben in den Prozessen wahrnehmen, Risiken besonders gut einschätzen können. Eine detaillierte unternehmensinterne Analyse hat auch zum Vorteil, dass die Risikoeinschätzung bzw. die Relevanz der Risiken über verschiedene Geschäftsbereiche ermittelt werden kann und sich so ein detailliertes Ergebnis ergibt, das bei einer gezielten Allokation der Steuerungsmaßnahmen herangezogen werden kann. Bedingt durch den unterschiedlichen strategischen Gehalt der Wissensrisiken und Steuerungsmaßnahmen ist auch der Einbezug von Führungskräften und Mitarbeitern, die operativen Tätigkeiten nachgehen, zu empfehlen, da eine multiperspektivische Betrachtung möglich wird und potentielle Umsetzungsprobleme etc. identifiziert werden können. Auf diese Weise können Austauschbeziehungen aufgedeckt werden, die es bei der Steuerung zu beachten gilt. Eine breite unternehmensinterne Erhebung kann zudem auch zur Identifikation weiterer Steuerungsmaßnahmen und Wissensrisiken sowie zur Identifikation von Varianten beitragen. Aus diesem Grund wird in nachfolgendem Abschnitt, der in den Abschnitten 5.10.2-5.10.4 hergeleitete Katalog an Steuerungsmaßnahmen, vor den Ergebnissen der empirischen Studie reflexiv betrachtet und dabei insbesondere auf zusätzliche Steuerungsmaßnahmen sowie Varianten zu bestehenden Steuerungsmaßnahmen eingegangen.

7.7 Reflexive Betrachtung der Steuerungsmaßnahmen

Im Rahmen der verschiedenen empirischen Studien wurden seitens der Interviewpartner Steuerungsmaßnahmen genannt, die über die im Interviewleitfaden erfassten Maßnahmen hinausgehen. So wurden als Maßnahmen die Dokumentation von Wissen, Personalentwicklung, Sensibilisierung der Mitarbeiter, Schaffung von Rollen und Mitarbeiterbindung genannt. Die Maßnahmen korrespondieren dabei mit den aus der Literatur hergeleiten Maßnahmen (siehe Abschnitte 5.10.2-5.10.4) und bestätigen somit deren Relevanz. Weiterhin wurden im Rahmen der Interviews Varianten zu den Steuerungsmaßnahmen, die Gegenstand des Interviewleitfadens sind, angeführt. Diese beiden Sachverhalte stellen eine qualitative Ergänzung des Katalogs an Steuerungsmaßnahmen dar und werden nachfolgend zu einer reflexiven Betrachtung des Katalogs an Steuerungsmaßnahmen herangezogen.

- **Dokumentation**: Im Rahmen der breiten Studie wurde die Dokumentation von Wissen (siehe auch SO17) von 16 Unternehmen genannt und als besonders relevant eingestuft (siehe Abschnitt 7.2.1). Aus den Telefoninterviews ergab sich in diesem Kontext, dass gerade durch die Dokumentation verschiedenen Wissensverlusten entgegengewirkt werden kann. Als spezieller Typ können

im Rahmen von Projekten Lessons Learned erstellt werden (siehe Abschnitt 7.6.2). Eine technische Umsetzung der Dokumentation, die auch zur Verbreitung dokumentierten Wissens dient, stellen Wissensdatenbanken dar (siehe Abschnitt 7.6.2).

- **Personalentwicklung**: Darüber hinaus wurde Personalentwicklung im Rahmen der breiten Studie von 11 Unternehmen genannt. Diese Steuerungsmaßnahme wurde zudem in den beiden vertiefenden Studien angeführt und ist auch Gegenstand der literaturbasierten Steuerungsmaßnahmen (siehe SO12). Eine gezielte Personalentwicklung kann in diesem Kontext dazu beitragen, dass Wissensrisiken, die auf mangelnde Kompetenzen zurückgehen, begrenzt werden. In einem Telefoninterview (C) wurde auch thematisiert, dass der Personalentwicklung bzgl. der Vermittlung sicherheitsrelevanter Kenntnisse eine hohe Bedeutung zukommt. Weiterhin wurde durch zwei Ansprechpartner[338] angeführt, dass Mitarbeiter des Unternehmens nach erfolgter Weiterbildung verpflichtet sind, dieses Wissen an die jeweiligen Kollegen weiterzugeben. Als Varianten wurden hierzu die Erstellung einer einseitigen Zusammenfassung sowie Präsentationen vor den jeweiligen Kollegen genannt.
- **Sensibilisierung der Mitarbeiter**: Sowohl in den vertiefenden Studien als auch in der breiten Studie wurde die Sensibilisierung der Mitarbeiter angeführt, wobei im Rahmen letztgenannter eine siebenfache Nennung erfolgte. Der Interviewpartner in Unternehmen C begründete die Bedeutung dieser Maßnahme damit, dass diese Art Risiken eine starke personelle Komponente aufweisen und somit der entsprechende Einbezug der Mitarbeiter unerlässlich ist.
- **Schaffung von Rollen**: Darüber hinaus wurde in der breiten Studie von fünf Interviewpartnern als zusätzliche Steuerungsmaßnahme die Schaffung von organisatorischen Rollen genannt. Dieser Sachverhalt ist auch Gegenstand der vertiefenden unternehmensübergreifenden Studie, nach der bei der Implementierung der Steuerung von Wissensrisiken in Unternehmen eine Rollen geschaffen werden sollten, die mit den verschiedenen Aspekten, wie z.B. IT, Personal, Werkschutz oder gewerbliche Schutzrechte, befasst sind[339].
- **Mitarbeiterbindung**: Im Rahmen der breiten Studie wurde die Mitarbeiterbindung in drei Fällen als weitere Steuerungsmaßnahme genannt. Auch im Rahmen der vertiefenden unternehmensinternen Studie wurde dieser Aspekt als Möglichkeit genannt, um fluktuationsbedingten Wissensverlusten entgegenzuwirken. Weiterhin wurde angeführt, dass diese Maßnahme auch zum gezielten Aufbau des akquisitorischen Potentials beitragen kann, indem u.a. eine gerechte Vergütung, Aufstiegschancen und ein gutes Arbeitsklima forciert werden. Diese Maßnahme ist auch Gegenstand der theoriebasierten Herleitung (siehe SO10).

[338] Diese Aussagen wurden von Unternehmen A sowie einem Ansprechpartner der breiten Studie gemacht.
[339] Dieser Aspekt wird nochmals gesondert bei der Betrachtung der Implementierung in Abschnitt 8.3 aufgegriffen.

Im Rahmen der vertiefenden Studie wurden darüber hinaus noch Varianten der im Interviewleitfaden einbezogenen Steuerungsmaßnahmen identifiziert, die interessante Aspekte aufweisen und nachfolgend dargestellt werden.

- **Klassifikation von Wissen**: Im Hinblick auf die Klassifikation von Wissen wurde in den vertiefenden Studien eine Variante angeführt, die der hohen Dynamik von Wissen bzw. der hohen Volatilität der Themengebiete Rechnung trägt. Demnach sollten seitens der Geschäftsführung bzw. des obersten Führungskreises, der beispielsweise das Managementteam und die Geschäftsbereichsleiter einschließt, in regelmäßigen Abständen neu definiert werden, welches Wissen als vertraulich gilt. Auf dieser Basis könnten dann die jeweiligen Projektleiter bzw. Prozessverantwortlichen auf der operativen Ebene definieren, welche Geheimhaltungsanforderungen auf der Ebene der Projekte / Prozesse bestehen. In einem Vertiefungsinterview (Ib) wurde angeführt, dass derartige Absprachen jeweils Gegenstand der wöchentlichen Sitzung des Managementteams sind und davon ausgehend die jeweiligen Projektleiter Anforderungen an die Mitarbeiter weitergeben.
- **Geheimhaltungsvereinbarungen**: Im Rahmen eines Vertiefungsinterviews (Ib) wurde darauf hingewiesen, dass im Hinblick auf die Geheimhaltung einer entsprechenden Erklärung der Gründe für das Geheimhaltungserfordernis von Bedeutung ist, um die Loyalität der Mitarbeiter durch Transparenz sicherzustellen. So wird es als essentiell erachtet, dass den Mitarbeitern vermittelt wird, aus welchen Gründen Wissen geheim zu halten ist, da so Vertrauen geschaffen wird und dies zur Loyalität der Mitarbeiter positiv beiträgt (siehe SR1).
- **Wissenstransferrichtlinien**: Analog zur Klassifikation von Wissen unterliegen auch Wissenstransferrichtlinien einer besonderen Dynamik. Im Rahmen der vertiefenden unternehmensinternen Studie (siehe Abschnitt 7.6) und durch den Ansprechpartner in Unternehmen Ib wurde angeregt, dass dieser Dynamik nur dann effizient Rechnung getragen werden kann, wenn ausgehend von einer unternehmensweiten Direktive der Geheimhaltungsbedarf bzw. die Transferierbarkeit des Wissens auf Projektebene seitens der Projektleiter definiert wird. Dies hat zum Vorteil, dass diese Mitarbeiter die unternehmensweiten Vorgaben kennen und über ausreichend Problemnähe verfügen, um derartige Vorgaben für die konkreten Sachverhalte zu machen (siehe SO6).
- **Zugriffsrechtevergabe**: Im Hinblick auf die Vergabe von Zugriffsrechten wurde durch den Ansprechpartner in Unternehmen IIIb angeregt, dass sichergestellt werden muss, dass derartige Beschränkungen nicht umgangen werden können. Somit ist die Vergabe von Zugriffsrechten durch weitere Richtlinien, wie z.B. technische Nutzungsbeschränkungen oder Regelungen zur Weitergabe von Passwörtern, zu flankieren (siehe hierzu auch SO1, ST8).
- **gewerbliche Schutzrechte**: Im Rahmen der vertiefenden unternehmensinternen Studie (siehe Abschnitt 7.6) wurde zudem angemerkt, dass gerade der Bereich der gewerblichen Schutzrechte durch eine hohe Komplexität charakterisiert ist. Daher ist es erforderlich, den bloßen Einsatz die-

ser Steuerungsmaßnahme durch den Einsatz von Rollen zu flankieren, die Transparenz in Bezug auf die Anmeldung von Schutzrechten oder dem Umgang mit Verletzungen schaffen (siehe auch SR6).

Insgesamt werden durch die qualitativen Anmerkungen fünf Steuerungsmaßnahmen, die nicht Gegenstand des Interviewleitfadens waren, aber im Maßnahmenkatalog (siehe Abschnitte 5.10.2-5.10.4) enthalten sind, bestätigt. Weiterhin konnten fünf werthaltige Varianten zu den 13 in der Studie betrachteten Steuerungsmaßnahmen gewonnen werden. Bei der Ergreifung von Steuerungsmaßnahmen des Katalogs können diese Erkenntnisse berücksichtigt werden.

7.8 Zusammenfassung und Diskussion

Nach der Erläuterung der Stichprobenstatistik (7.1) wurde im Rahmen von Abschnitt 7.2 eine deskriptive Auswertung der einzelnen Variablen vorgenommen. Dazu wurden Mittelwertvergleiche zwischen verschiedenen Teilstichproben herangezogen, wobei signifikante Abweichungen auch der Basis von T-Tests bei einem adjustierten Signifikanzniveau nach Bonferroni-Holm ermittelt wurden. Hinsichtlich des Vergleichs zwischen mittelständischen und Großunternehmen zeigte sich, dass letztere in der Relation signifikant geringer von Risiken im Kontext des Wissensverlustes und der Wissensdiffusion betroffen sind. Im Falle des Wissensverlustes sind Großunternehmen signifikant weniger von durch die Wissensrisiken der Nichtdokumentation im Tages- und Projektgeschäft betroffen.

In Bezug auf die Teilstichproben produzierender und dienstleistungsorientierter Unternehmen bestehen keine signifikanten Unterschiede. Deutliche Unterschiede ergaben sich allerdings zwischen Unternehmen, die RM- und WM-Initiativen implementiert haben, im Vergleich zu Unternehmen ohne diese Maßnahmen. So implementieren Unternehmen mit Maßnahmen in beiden Bereichen neun der 13 Steuerungsmaßnahmen umfassender und weisen in Bezug auf die Konzepte Wissensverlust, Wissenstransfer und Wissensqualität vielfach signifikant geringere Wissensrisikoausprägungen auf[340].

In Abschnitt 7.3 wurden die Einflüsse der 13 Steuerungsmaßnahmen auf die abhängigen Konzepte untersucht, da bei der Konzeption der Studie negative Einflüsse der Maßnahmen vermutet wurden, was insbesondere an den Austauschbeziehungen zwischen den Konzepten Wissensdiffusion und Wissenstransfer deutlich wird. Die Analyse führte zu dem Ergebnis, dass keine der Steuerungsmaßnahmen signifikant mit einer höheren Wissensrisikoausprägung in Zusammenhang steht. Dabei ist insbesondere hervorzuheben, dass die beiden Maßnahmen Wissenstransferrichtlinien und Begrenzung der Interaktion entgegen der Annahmen im Vorfeld der Studie keine negativen Effekte auf den Erfolg des Wissenstransfers haben. Ebenso stehen umfassender implementierte IT-Sicherheitsrichtlinien ebenfalls nicht in Zusammenhang miteinem geringeren Erfolg des Wissenstransfers.

[340] Für Details siehe Abschnitt 7.2.7.

Basierend auf den Daten der breiten Studie wurden in Abschnitt 7.4 durch eine Clusteranalyse, die auf einer Faktorenanalyse aufsetzt, vier Gruppen an Unternehmen identifiziert und in einer vertiefenden Studie je zwei Unternehmen je Cluster erneut zu spezifischen Zusammenhängen befragt. Weiterhin wurden vier Unternehmen, die durch vergleichsweise positive Ausprägungen über die vier abhängigen Konzepte charakterisiert sind, erneut befragt (siehe Abschnitt 7.5). Dabei sind insbesondere die Erkenntnisse in Bezug auf unternehmensinterne und -externe Einflussfaktoren hervorzuheben. Diese können herangezogen werden, um hohe oder niedrige Wissensrisikoausprägungen zu erklären.

Neben der vertiefenden unternehmensübergreifenden Studie wurde auch ein Unternehmen vertiefend untersucht (7.6), wobei 66 Führungskräfte und Mitarbeiter aus verschiedenen produktionsnahen und kaufmännischen Geschäftsbereichen befragt wurden. Durch diese Analyse wurde einerseits die Spannweite der Einschätzung von Wissensrisiken über verschiedene Geschäftsbereiche und zwischen den Mitarbeitergruppen aufgezeigt. Im Vergleich zur breiten Studie bestehen vergleichsweise weniger signifikante Abweichungen zwischen den Teilstichproben, was auf eine in der Relation homogenere Einschätzung der Risiken zurückgeführt werden kann. Diese homogene Einschätzung zeigt sich insbesondere bei den Konzepten Wissenstransfer und -qualität. Insgesamt ist eine breite unternehmensinterne Analyse werthaltig, da bedingt durch die operative Ausrichtung auf die Ebene der Geschäftsprozesse insbesondere auch Mitarbeiter, die im Tagesgeschäft Aufgaben in den Prozessen wahrnehmen, Risiken besonders gut einschätzen können. Weiterhin kann eine Analyse über verschiedene Geschäftsbereiche ein differenziertes Bild zu Wissensrisikopotentialen liefern und so das punktuelle Ergreifen von Maßnahmen unterstützen.

Bedingt durch die qualitativen Anmerkungen in den Interviews und die offenen Fragen im Interviewleitfaden konnten über die in der Studie eingeschlossenen 13 Steuerungsmaßnahmen weitere Maßnahmen identifiziert werden (7.7). Dadurch konnten einige der in den Abschnitten 5.10.2-5.10.4 auf Basis der Theorie hergeleiteten Maßnahmen empirisch reflektiert werden. Weiterhin wurden zu fünf der 13 in der Studie eingeschlossenen Steuerungsmaßnahmen basierend auf qualitativen Anmerkungen Variationen identifiziert, die bei der Ergreifung der Steuerungsmaßnahmen berücksichtigt werden können. Basierend auf den aus der Literatur und der empirischen Studie gewonnenen Erkenntnisse werden im folgenden Kapitel Handlungsempfehlungen erarbeitet.

8 Handlungsempfehlungen

Nach Operationalisierung und empirischer Betrachtung des Konzeptes Wissensrisiko und der entsprechenden Teilkonzepte werden in diesem Kapitel Handlungsempfehlungen erarbeitet, die sich sowohl auf die theoretischen, als auch auf die empirischen Erkenntnisse stützen. So hat sich im Verlauf der Studie gezeigt, dass die Klassifikation von wissensbezogenen Ressourcen dann bedeutend ist, wenn definiert werden soll, welche Steuerungsmaßnahmen zu ergreifen sind bzw. welche dieser Ressourcen zu schützen sind. Aus diesem Grund werden in diesem Kapitel eine entsprechende Heuristik zur Klassifikation dieser Ressourcen und korrespondierende Normstrategien entwickelt, die auf der vertiefenden empirischen Studie basieren (siehe 8.1). Darüber hinaus wird im Rahmen dieses Kapitels ein Handlungskonzept zum Einsatz der Steuerungsmaßnahmen entwickelt, das Potentiale der Steuerungsmaßnahmen, die Steuerbarkeit von Wissensrisiken, potentielle Austauschbeziehungen sowie externe Einflussfaktoren zusammenfassend betrachtet (siehe 8.2). Da das erarbeitete Konzept einer Verankerung in der Aufbau- und Ablauforganisation bedarf, wird auf Basis der vertiefenden Studie ein Implementierungskonzept entwickelt, das Gegenstand von Abschnitt 8.3 ist.

8.1 Heuristik zur Klassifikation von Wissen und Normstrategien

Sowohl bei der theoretischen Analyse[341] als auch bei der Durchführung der empirischen Studie hat sich gezeigt, dass die Klassifikation von Wissen eine Voraussetzung für die effiziente Umsetzung weiterer Steuerungsmaßnahmen ist und diesen eine Richtung vorgibt. Somit ist die Klassifikation von Wissen z.B. erforderlich, wenn es zu bestimmen gilt, welches Wissen geheim zu halten ist, welches Wissen im Rahmen von Kooperationen weitergegeben werden kann oder für welches Wissen gewerbliche Schutzrechte ergriffen werden sollen. Aufgrund dieser Bedeutung wird in folgendem Abschnitt eine Heuristik zur Klassifikation von Wissen erarbeitet, auf deren Basis Unternehmen eine Einordnung wissensbezogener Ressourcen vornehmen und so Handlungsbedarfe in Bezug auf den Schutz dieser Ressourcen ableiten können. Die Heuristik basiert auf Faktoren zur Bestimmung des Wertes der wissensbezogenen Ressourcen, deren Ableitung sowohl auf die Erkenntnisse aus der Empirie[342] als auch auf die Literaturanalyse zurückgeht.

Die Faktoren werden zwei Dimensionen zugeordnet und betreffen zum einen den unternehmensinternen und zum anderen den unternehmensübergreifenden Wert dieser Ressourcen[343]. Darüber hinaus bestehen noch weitere Faktoren, die die Charakteristika wissensbezogener Ressourcen widerspiegeln

[341] Siehe hierzu Abschnitt 5.9.1.

[342] Im Rahmen der vertiefenden unternehmensübergreifenden Studie wurden 12 Unternehmen befragt, welche Kriterien zur Klassifikation von Wissen herangezogen werden können. Siehe hierzu auch den Interviewleitfaden für die vertiefende Studie in Anhang A 2.

[343] Ein erster Ansatz zur Klassifikation wurde im Rahmen einer vom Autor mitbetreuten Diplomarbeit an der Universität Halle-Wittenberg entwickelt (Hain 2007).

und die Anwendbarkeit durch Dritte und somit den Schutzbedarf beeinflussen. Diese Faktoren haben folglich einen kontrollierenden Charakter. Nachfolgend werden die Dimensionen erörtert und in ein Portfolio zur Ableitung von Normstrategien überführt.

Unternehmensinterner Wert: Folgende Faktoren können herangezogen werden, um den unternehmensinternen Wert wissensbezogener Ressourcen zu bestimmen.

- **Wertschöpfungsbeitrag**: Im Rahmen der vertiefenden Interviews wurde von sechs Ansprechpartnern (Ia, Ib, IVa, IVb, A, D) angeführt, dass als ein Kriterium zur Klassifikation von Wissen der Wertschöpfungsbeitrag der wissensbezogenen Ressourcen herangezogen werden kann. So betonten zwei Ansprechpartner aus produzierenden Unternehmen (Ia, IVb), dass die Produktentwicklung zur Wertschöpfung beiträgt bzw. eine Kernkompetenz des Unternehmens darstellt und daher Wissen in diesem Kontext Priorität beim Schutz aufweist. Ein Ansprechpartner (D) hob hervor, dass sehr gute Lieferantenbeziehungen und die Qualität der Zusammenarbeit mit den Lieferanten (z.B. in Bezug auf Liefertreue, Lieferzeit etc.) einen Wettbewerbsvorteil des Unternehmens ausmacht. Aus diesem Grund wird Wissen, das die Lieferanten betrifft, streng geheim gehalten. Auch in der Literatur wird diesem Faktor Bedeutung beigemessen. So empfehlen einige Autoren, den sensitiven Umgang mit Informationen bzw. Wissen am Beitrag zur Wertschöpfung bzw. zum Unternehmenserfolg festzumachen (McGonagle, Vella 2004, 74f)[344]. Folglich ist der Schutzbedarf der wissensbezogenen Ressourcen umso höher einzustufen, umso mehr diese zu den Kernkompetenzen, der Differenzierung gegenüber Wettbewerbern und somit zur Erzielung von Wettbewerbsvorteilen beitragen.
- **Innovationsbeitrag**: Im Rahmen der Vertiefungsinterviews wurde von vier Ansprechpartnern (IIa, IIIb, IVb, D) darauf hingewiesen, dass Schutzbedarf insbesondere dann entsteht, wenn das Wissen positiv zur Innovationsfähigkeit des Unternehmens beiträgt. Dieser Faktor ist dann von Relevanz, wenn Unternehmen in Branchen agieren, in denen die Produktlebenszyklen und die Halbwertszeit des Wissens eher gering sind und Innovationen eine hohe Bedeutung bzgl. der Erzielung der Umsätze aufweisen. Auch in der Literatur wird der Schutz von Wissen mit einer hohen Aktualität besonders empfohlen, wobei die Halbwertszeit des Wissens einen regulierenden Einflussfaktor darstellt (Kern et al. 1998, 10; McGonagle, Vella 2004, 74f). Folglich nimmt der unternehmensinterne Wert mit steigendem Innovationsbeitrag zu.
- **Kundenfokus**: Ein weiterer Faktor, der durch sieben der zwölf Interviewpartner (IIb, IIIa, IIIb, IVa, A, C, D) im Rahmen der vertiefenden Studie genannt wurde, ist der Schutz von Inhalten, die die Kunden des Unternehmens betreffen. Eine Verletzung der aus der Zusammenarbeit mit Kunden erwachsenden Geheimhaltung kann Reputationsschäden zur Folge haben. Dieses Wissen be-

[344] Zur Ermittlung des Wertbeitrags können die einzelnen wissensbezogenen Ressourcen mit Hilfe einer Wertbeitragsmatrix in Beziehung gesetzt werden. Siehe hierzu (Carlucci, Schiuma 2006, 39f).

trifft z.B. konkrete Aufträge, Konzepte, Prozesse oder Produkte der Kunden. Aufgrund dieser Bedeutung wird in den Unternehmen kundenrelevantes Wissen sensitiv behandelt, wobei der unternehmensinterne Wert der Ressourcen mit steigendem Kundenbezug zunimmt.

- **Schadenspotential**: Als alternativer Ansatz, der in der Literatur empfohlen wird, kann unternehmensseitig geschätzt werden, welcher Schaden aus einer unerwünschten Diffusion oder durch den Verlust der wissensbezogenen Ressourcen entstehen würde. Als Anhaltspunkt können die Kenntnisnahme durch Wettbewerber und die potentielle Einbuße von Wettbewerbsvorteilen, der Schaden aus mangelnder Verfügbarkeit, Wiederherstellungskosten, die Schäden aus der Verletzung von Regularien (z.B. Basel II, SOX) oder Gesetzen (z.B. KonTraG, BDSG) sowie Reputationsverluste und Vertrauensverluste herangezogen werden (Gordon, Loeb 2001, 74; Peltier 2001, 5; Queensland 2001, 22; Yapp 2003, 173f)[345]. Umso höher das Schadenspotential ist, umso höher ist auch der unternehmensinterne Wert der wissensbezogenen Ressourcen und somit deren Schutzbedarf.

Insgesamt dienen die Faktoren als Anhaltspunkte zur unternehmensinternen Bewertung und sind komplementär zu verstehen. Sind mehrere Faktoren gleichzeitig erfüllt, so erhöht dies konsequenterweise den Schutzbedarf der entsprechenden wissensbezogenen Ressourcen.

Unternehmensübergreifender Wert: Neben unternehmensinternen Faktoren wird der Handlungsbedarf auch durch eine Reihe unternehmensübergreifender Faktoren beeinflusst, die nachfolgend detailliert werden.

- **Nachfrage knapper Ressourcen**: Der unternehmensübergreifende Wert der wissensbezogenen Ressourcen ergibt sich daraus, wie stark diese Ressourcen durch Unternehmen nachgefragt werden und inwiefern sie auf den entsprechenden Märkten verfügbar sind. Sind stark nachgefragte Ressourcen zugleich knapp, erhöht dies deren unternehmensübergreifenden Wert. Als Beispiel für eine derartig werterhöhende Knappheit führte ein Interviewpartner (Ib) an, dass in der Branche ein Fachkräftemangel vorliegt und es deswegen zum Teil sehr schwer ist, qualifizierte Mitarbeiter mit knappen stark nachgefragten Kompetenzen an das Unternehmen zu binden bzw. zu gewinnen[346].
- **Entwicklungsaufwand**: Weiterhin kann der unternehmensübergreifende Wert der wissensbezogenen Ressourcen auch am Aufwand, der für Konkurrenten oder Dritte entsteht, wenn diese das Wissen entwickeln möchten, festgemacht werden. Analog zur Knappheit nimmt bei hohem Ent-

[345] In diesem Kontext wurde auch durch die Interviewpartner angeführt, dass der Handlungsbedarf durch die gesetzliche Regulierung beeinflusst wird. So sind personenbezogene Daten nach BDSG zu schützen, für die erfolgreiche Zertifizierung bestimmte Auflagen zu erfüllen oder nach verschiedenen Regularien wie Basel II, Sarbanes-Oxley oder KonTraG einzuhalten. Je mehr das dokumentierte Wissen diese Bereiche betrifft, umso sensitiver sollte das Unternehmen damit umgehen.

[346] Im umgekehrten Fall legte ein Interviewpartner (IIIa) dar, dass die Qualifikationen, über die die Mitarbeiter verfügen, zum Teil sehr knapp sind, aber aufgrund ihrer hohen Spezifität die Nachfrage auf dem Arbeitsmarkt gering ist.

wicklungsaufwand die Bereitschaft Dritter zu, Maßnahmen (z.B. Abwerbung, Competitive Intelligence, Reverse Engineering) zu ergreifen, um sich wissensbezogene Ressourcen anzueignen[347].

- **Anwendbarkeit**: Neben dem Entwicklungsaufwand wird der unternehmensübergreifende Wert der wissensbezogenen Ressourcen auch dadurch beeinflusst, inwieweit diese Ressourcen in anderen Unternehmen angewandt werden können. Die Anwendbarkeit wird zum einen dadurch bestimmt, welche Eigenschaften die wissensbezogenen Ressourcen in Bezug auf Kontexteinbettung, Spezifität und Kodifizierung aufweisen. Zum anderen beeinflussen auch die Fähigkeiten der Unternehmen, externes Wissen zu akquirieren und zu assimilieren, den unternehmensübergreifenden Wert[348].

Dieses Kriterium wird zudem durch die Charakteristika von Wissen beeinflusst, die je nach Ausprägung die Anwendbarkeit durch Dritte erschweren bzw. gänzlich verhindern.

- **Kontexteinbettung**: Wissensbezogene Ressourcen unterscheiden sich im Hinblick auf ihre Abhängigkeit von anderem Wissen (Zander, Kogut 1995, 77,82; Matusik, Hill 1998, 684f). So ist für die Anwendung von Wissen anderes Wissen erforderlich. Fehlt dieses Wissen oder ist es nicht in ausreichendem Maße vorhanden, wird die Anwendbarkeit durch Dritte erschwert.
- **Spezifität**: Einen weiteren Einflussfaktor in Bezug auf die Anwendbarkeit stellt die Spezifität des Wissens dar. So wird beispielsweise Wissen entwickelt, das auf Problemstellungen bezogen ist, die eine gewisse Einzigartigkeit bzw. einen starken Unternehmensbezug aufweisen, wodurch eine Adaption außerhalb des Unternehmens erschwert bzw. verhindert wird (von Krogh, Roos 1996, 45; Child 2001, 661; Jacob, Ebrahimpur 2001, 84). Die hohe Spezifität des Wissens kann zur Folge haben, dass zwar dessen unternehmensinterner Wert hoch ist, aber im unternehmensübergreifenden Kontext nur ein geringer Marktwert besteht. Im Rahmen der Vertiefungsinterviews führte ein Ansprechpartner an, dass die Qualifikationen der Mitarbeiter so spezifisch sind, dass sie auf dem Arbeitsmarkt nahezu keinen Wert aufweisen (IIIa)[349]. Weiterhin führten Ansprechpartner in zwei Unternehmen (IIIa, D) an, dass die Lösungen bzw. die Produkte, die für die Kunden erstellt werden, so spezifisch und an deren Anforderungen angepasst sind, dass ein effizienter Einsatz in anderen Unternehmen als nicht relevant angesehen wird.
- **Kodifizierung**: Weiterhin nimmt der Grad der Kodifizierung Einfluss auf die Anwendbarkeit von Wissen. So kann Wissen, das losgelöst von Personen in verschiedensten Dokumentationen (z.B. Konzepten, Patenten, Handbüchern) oder Datenbanken inkorporiert ist, vergleichsweise einfacher durch Dritte genutzt werden.

[347] Siehe hierzu auch (McGonagle, Vella 2004, 74f).
[348] Diese Fähigkeiten können zusammenfassend auch als Absorptive Capacity umschrieben werden (Cohen, Levinthal 1990, 499ff).
[349] Im konkreten Fall handelte es sich um ein Unternehmen, das in einer Marktnische im Formenbau tätig ist.

Die Faktoren sind in nachfolgender Abb. 42 integriert und bilden die Basis zur Klassifikation von Wissen und zur Ableitung von Normstrategien.

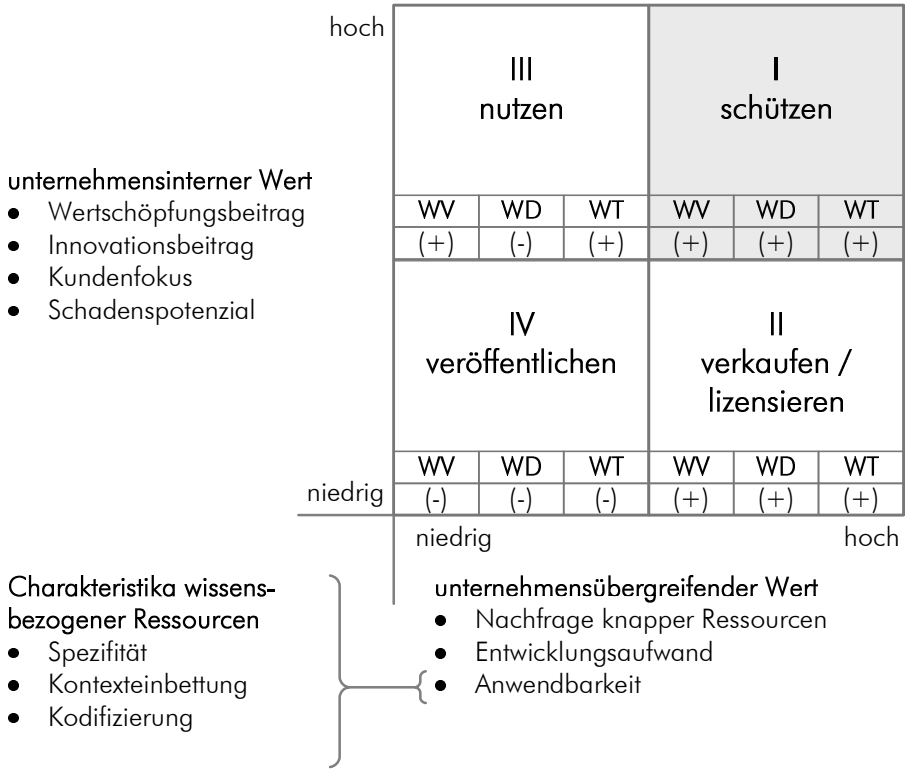


Abb. 42 Heuristik zur Klassifikation von Wissen und korrespondierende Normstrategien

Auf Basis der Einordnung der wissensbezogenen Ressourcen bzw. Themen entlang der beiden Dimensionen lassen sich vier Normstrategien in Bezug auf den risikobewussten Umgang mit Wissen ableiten, wobei die Einordnung vor dem Hintergrund der Charakteristika der wissensbezogenen Ressourcen zu reflektieren ist, da diese die Anwendbarkeit dieser Ressourcen beeinflussen. Je Normstrategie sind in Abb. 42 zudem die Handlungsbedarfe in Bezug auf Steuerungsmaßnahmen abgetragen, die die Verminderung von Wissensrisiken in Bezug auf die Konzepte Wissensverlust (WV), Wissensdiffusion (WD) und Wissenstransfer (WT) betreffen. Im Falle eines (+) in Abb. 42 sollten Maßnahmen in diesem Bereich ergriffen werden, während im Falle eines (-) die Ergreifung von Steuerungsmaßnahmen nicht oder nur in geringem Umfang erforderlich ist. Maßnahmen zur Erhöhung der Wissensqualität sollten unabhängig vom unternehmensinternen und -übergreifenden Wert in jedem Fall ergriffen werden, da sowohl bei interner Nutzung als auch beim Verkauf oder der Veröffentlichung von Wissen (z.B. im Hinblick auf die Gewährleistung der Reputation des Unternehmens) eine hohe Qualität sichergestellt werden sollte. Je nach Einordnung der wissensbezogenen Ressourcen bestehen unterschiedliche Anforderungen an die Steuerung. Entsprechend des Umfangs an Steuerungsmaß-

nahmen bzw. des Schutzbedarfes werden nachfolgend die Quadranten absteigend nach ihrem Schutzbedarf erläutert.

- **(I) schützen**: Bei einem hohen unternehmensinternen und zugleich hohen unternehmensübergreifenden Wert der wissensbezogenen Ressourcen ist ein umfassender Schutz dieser Ressourcen aus Risikoaspekten zu empfehlen. So sollten Maßnahmen ergriffen werden, die dazu beitragen, die Eintrittswahrscheinlichkeit eines Verlustes dieser Ressourcen zu reduzieren. Darüber hinaus ist v.a. die Ergreifung von Steuerungsmaßnahmen, die die Reduktion des Risikoerwartungswertes einer Diffusion zum Ziel haben, zu empfehlen, da aufgrund des Wertes für andere Unternehmen eine Erosion der Wettbewerbsposition erfolgen kann. Im Hinblick auf den Wissenstransfer sollte beachtet werden, dass dieses Wissen besonders werthaltig ist und aus diesem Grund nicht an Dritte weitergegeben werden sollte.
- **(II) verkaufen / lizenzieren**: Weisen die wissensbezogenen Ressourcen einen geringen unternehmensinternen Wert auf, während der unternehmensübergreifende Wert hoch ist, so kann ein Verkauf bzw. eine Lizenzierung empfohlen werden. Eine derartige Situation kann sich beispielsweise dann ergeben, wenn Unternehmen ihre strategische Ausrichtung geändert haben und Wissen zu bestimmten Themengebieten zukünftig weniger genutzt wird. Durch eine Lizenzierung kann zur Weiterentwicklung der wissensbezogenen Ressourcen beigetragen werden, in die aufgrund ihres vergleichsweise geringeren unternehmensinternen Wertes weniger investiert wird. Um Erlöse aus dem Verkauf oder der Lizenzierung dieser für Dritte werthaltigen wissensbezogenen Ressourcen sicherzustellen, sollten Steuerungsmaßnahmen eingesetzt werden, die primär auf die Vermeidung der Diffusion und des Verlustes bzw. auf die Reduktion der entsprechenden Eintrittswahrscheinlichkeit abzielen[350]. Im Falle der Lizenzierung sollten weiterhin Maßnahmen zur Verbesserung des Wissenstransfers zwischen Lizenzgeber und -nehmer ergriffen werden, um an der Weiterentwicklung der wissensbezogenen Ressourcen zu partizipieren.
- **(III) nutzen**: Im Falle eines hohen unternehmensinternen und eines geringen unternehmensübergreifenden Wertes der wissensbezogenen Ressourcen ist deren Nutzung unter vergleichsweise geringen Sicherheitsvorkehrungen zu empfehlen. So sollten die Steuerungsmaßnahmen primär darauf ausgerichtet sein, zu gewährleisten, dass die wissensbezogenen Ressourcen nicht verloren gehen und der Wissenstransfer mit den Partnern möglichst effizient abläuft. Maßnahmen zur Begrenzung der Diffusion sind dabei von geringerer Relevanz, da diese Ressourcen einen vergleichsweise geringen unternehmensübergreifenden Wert aufweisen.
- **(IV) veröffentlichen**: Wenn sowohl der unternehmensinterne als auch der -übergreifende Wert der wissensbezogenen Ressourcen niedrig sind, so kann als Normstrategie deren Veröffentlichung

[350] In diesem Kontext kann auch auf die Variante der offensiven Nutzung des intellektuellen Kapitals hingewiesen werden (siehe Abschnitt 2.3.1), wie sie durch Sullivan in Betracht gezogen wird (Sullivan 1999, 137).

empfohlen werden, da so potentiell eine Erweiterung dieses Wissens erfolgt und somit möglicherweise eine Werterhöhung eintritt. So kann beispielsweise die Offenlegung von Spezifikationen oder Softwarecode zu einer Erweiterung durch Dritte führen, die ihrerseits wiederum werthaltig für das Unternehmen sein kann. Der Einsatz von Steuerungsmaßnahmen zum Schutz der wissensbezogenen Ressourcen dieser Kategorie ist nicht erforderlich.

Insgesamt weisen die Ressourcen in Quadrant I den höchsten Schutzbedarf auf, da sie sowohl für das Unternehmen als auch für andere Unternehmen werthaltig sind. Im Falle von Quadrant II ist die Werthaltigkeit für das Unternehmen vergleichsweise geringer, weshalb durch die Ergreifung der Schutzmaßnahmen primär Erlöse aus dem Verkauf oder der Lizenzierung sichergestellt werden sollen. Die wissensbezogenen Ressourcen in Quadrant III sind aufgrund mangelnden Wertes für andere Unternehmen nur in geringem Umfang von den Risiken der Diffusion betroffen. Dennoch ist sicherzustellen, dass die Ressourcen erhalten bleiben, um die Durchführung der Prozesse nicht zu hemmen. Letztlich weisen Ressourcen in Quadrant IV aufgrund ihrer vergleichsweise geringen Werthaltigkeit in Bezug auf beide Dimensionen einen geringen Schutzbedarf auf. Um die Verwendung der Heuristik zu verdeutlichen, werden im Folgenden je Feld Beispiele für Ressourcen angeführt, deren Einordnung in das Portfolio erläutert sowie Beispiele für Maßnahmen gegeben[351].

- **zu I) schützen**: Als Beispiel für wissensbezogene Ressourcen, die dem Quadranten „schützen“ zuzuordnen sind, können im Falle eines Industrieunternehmens aktuelle Konzepte zu neuen Produkten oder Prototypen genannt werden. Bezogen auf den unternehmensinternen Wert weisen sie einen hohen Innovationsbeitrag auf und gehen bei erfolgreicher Entwicklung mit einem hohen zukünftigen Beitrag zur Wertschöpfung einher. Handelt es sich um Entwicklungen, die ein hohes Marktvolumen aufweisen, dürfte auch die Nachfrage von Konkurrenzunternehmen hoch sein, da sie an diesem Volumen partizipieren wollen, wodurch sich der unternehmensübergreifende Wert erhöht. Ist das Unternehmen schon längere Zeit mit der Entwicklung des korrespondierenden Wissens befasst, so ist zudem der Entwicklungsaufwand für Konkurrenten hoch, wodurch die Risikopotentiale zunehmen. Die Anwendbarkeit wird durch die Spezifität, Kontexteinbettung und Kodifizierung determiniert und wirkt somit als kontrollierender Faktor. In einer derartigen Konstellation kann durch Konkurrenten versucht werden, Mitarbeiter, die über entsprechende Kompetenzen verfügen, abzuwerben oder sich die Entwicklungen durch Betriebsspionage anzueignen. Weiterhin besteht im Falle unternehmensübergreifender Produktentwicklungen die Gefahr, dass Wissen ungewollt abfließt, weshalb entsprechende Maßnahmen zur Kontrolle des Wissenstransfers ergriffen werden sollten, wobei eine zu rigide Kontrolle die Potentiale des Transfers hemmen könnte. Als Maßnahme kann die Mitarbeiterbindung (siehe SO10) erhöht werden, um so die Erwartungswerte

[351] Bei der Erläuterung der Normstrategien wird auf die aus der Literatur identifizierten und in den Abschnitten 5.10.2-5.10.4 dargestellten Steuerungsmaßnahmen verwiesen.

von Abwanderung und somit von Wissensverlusten und -diffusionen zu vermindern. Weiterhin können Maßnahmen zur Abwehr von Betriebsspionage (siehe SR5) ergriffen werden und Wissenstransferprozesse kontrolliert (siehe SO6) werden, um den Erwartungswert einer Wissensdiffusion zu senken. Im Rahmen der unternehmensübergreifenden Zusammenarbeit können vertrauensbildende Maßnahmen (siehe SO28) zu einer Verbesserung des Wissenstransfers beitragen und Kontrollen ergänzen.

- **zu II) verkaufen / lizenzieren**: Bedingt durch Innovation kann Wissen für ein Unternehmen an Aktualität oder Wert verlieren, was zur Folge hat, dass bestimmte Technologien oder Verfahren, die auf diesem Wissen basieren, durch das Unternehmen nicht mehr eingesetzt werden. Aus diesem Grund sind dessen Wertschöpfungs- und der Innovationsbeitrag und somit der unternehmensinterne Wert gering. Dennoch kann dieses Wissen für andere Unternehmen, die noch diese Technologien einsetzen, oder für andere Märkte von Relevanz sein, wodurch der unternehmensübergreifende Wert zunimmt. Ungeachtet des geringen unternehmensinternen Wertes sollten seitens des Unternehmens Steuerungsmaßnahmen zum Schutz ergriffen werden, wenn Erlöse aus dem Verkauf dieser wissensbezogenen Ressourcen sichergestellt werden sollen, da die Attraktivität für Dritte hoch ist. So sind im Konkreten Maßnahmen zur Vermeidung von Wissensverlusten (z.B. Schutz der IT-Systeme[352]) oder -diffusionen (z.B. Abwehr von Betriebsspionage[353]) zu ergreifen. Im Falle einer Lizenzierung können auch Maßnahmen zur Verbesserung des Wissenstransfers (z.B. SO28) zwischen Lizenznehmer und Lizenzgeber ergriffen werden, damit das Unternehmen an der Weiterentwicklung der Ressourcen durch den Lizenznehmer partizipiert.
- **zu III) nutzen**: Neben wissensbezogenen Ressourcen, die sich in Entwicklung befinden, und solchen, die bedingt durch Innovationen überholt sind, werden wissensbezogene Ressourcen, wie z.B. Produktpläne oder Beratungskonzepte, im Unternehmen genutzt und können somit einen hohen Wertschöpfungsbeitrag aufweisen. Darüber hinaus können die wissensbezogenen Ressourcen auch durch einen starken Kundenfokus charakterisiert sein. Werden beispielsweise Beratungskonzepte für Kunden entwickelt, liegen vielfach aufgrund der Analyse der Problemstellung umfassende Erkenntnisse zu Spezifikas des Kunden vor, die sensitiver Natur sind. Stehen diese Ressourcen nicht zur Verfügung, ist auch das Schadenspotential hoch, da diese Ressourcen in verschiedenen Prozessen zum Einsatz kommen und deren Durchführung bei Nichtverfügbarkeit gehemmt wird. Unternehmensübergreifend betrachtet können diese Ressourcen so spezifisch sein, dass sie von anderen Unternehmen nicht nachgefragt werden. Dies ist beispielsweise bei Unternehmen der Fall, die in Marktnischen tätig sind. Aufgrund des geringen unternehmensübergreifenden Wertes sind Maßnahmen zur Verminderung der Risiken aus Wissensdiffusion in geringem Umfang von Rele-

[352] Siehe ST1.
[353] Siehe SR5.

vanz. Vielmehr ist seitens des Unternehmens sicherzustellen, dass Wissensverluste vermieden werden. So können im Konkreten beispielsweise Nachfolger- (siehe SO18) und Vertreterregeln (siehe SO19) implementiert werden, um fluktuationsbedingten Wissensverlusten entgegenzuwirken. Weiterhin sollten im Falle einer unternehmensübergreifenden Zusammenarbeit Maßnahmen zur Verbesserung des Wissenstransfers, wie z.B. vertrauensbildende Maßnahmen (siehe SO28) oder Partnerbindung (siehe SO23), ergriffen werden, um die Potentiale aus dem Wissenstransfer so gut wie möglich zu nutzen.

- **zu IV) veröffentlichen**: Weiterhin kann im Unternehmen Wissen zu Produkten, Technologien oder Verfahren vorliegen, das sowohl unternehmensintern aufgrund eines geringen Wertschöpfungs- und Innovationsbeitrags als auch unternehmensübergreifend aufgrund einer geringen Nachfrage einen vergleichsweise geringen Wert aufweist. Als Beispiel kann Wissen zu Technologien genannt werden, das aufgrund der Standardisierung von konkurrierenden Technologien in der gesamten Branche einen geringen Wert aufweist. Durch die Veröffentlichung dieses Wissens besteht die Chance, dass eine Weiterentwicklung erfolgt. Mit Ausnahme der allgemeinen Maßnahmen zur Verbesserung der Wissensqualität sind keine Maßnahmen zum Schutz dieser Ressourcen erforderlich und im Hinblick auf eine gezielte Allokation der Steuerungsmaßnahmen auch nicht zu empfehlen.

Insgesamt kann eine grobe Einordnung der wissensbezogenen Ressourcen entlang dieser Dimensionen zur Bestimmung des Schutzbedarfes beitragen und somit insbesondere die gezielte und ökonomische Allokation von Steuerungsmaßnahmen ermöglichen. Unter Konzentration auf zu schützende Ressourcen wird nachfolgend das Handlungskonzept, durch das eine effiziente Steuerung erreicht werden soll, detailliert.

8.2 Handlungskonzept zum Einsatz von Steuerungsmaßnahmen

In das Handlungskonzept zum Umgang mit Wissensrisiken werden unterschiedliche Faktoren einbezogen. So wird zunächst analysiert, welche Potentiale die Steuerungsmaßnahmen aufweisen (8.2.1) und mit welchem Steuerungsbedarf die Wissensrisiken (8.2.2) einhergehen. Weiterhin bestehen Austauschbeziehungen beim Einsatz von Steuerungsmaßnahmen, die im Rahmen der qualitativen Angaben in den Interviews ermittelt wurden und beim Management von Wissensrisiken beachtet werden sollten (8.2.3). Schließlich konnten im Rahmen der breiten und vertiefenden Studien Einflussfaktoren identifiziert werden, die sich auf die Risikoausprägungen über die Konzepte hinweg und die erforderliche Intensität der Implementierung der Steuerungsmaßnahmen auswirken (8.2.4). Abschließend werden die für die Steuerung von Wissensrisiken relevanten Erkenntnisse dieses Abschnitts integriert betrachtet (8.2.5)

8.2.1 Potential der Steuerungsmaßnahmen

Zur Identifikation von Steuerungsmaßnahmen mit einem hohen Potential werden in diesem Abschnitt drei verschiedene Quellen herangezogen. So weisen auf der einen Seite diejenigen Steuerungsmaßnahmen, die von den 30 Unternehmen mit den positivsten Ausprägungen über die vier abhängigen Konzepte hinweg eingesetzt werden[354], möglicherweise ein hohes Potential auf. Zum Zweiten könnten die Maßnahmen präferiert herangezogen werden, denen durch die Unternehmen im Rahmen der breiten und vertiefenden Studie die höchste Bedeutung beigemessen wurde. Darüber hinaus hat die theoretische Analyse gezeigt, dass sich die Steuerungsmaßnahmen in Bezug auf die Anzahl steuerbarer Wissensrisiken potentiell unterscheiden. Demnach dürften diejenigen Maßnahmen, durch die sich vergleichsweise viele Wissensrisiken reduzieren lassen, ein hohes Potential aufweisen. Daher werden zur empirischen Fundierung von Handlungsempfehlungen zur effizienten Steuerung die vier Unternehmen (A-D) genauer betrachtet, die in Bezug auf die Wissensrisiken, die zur Operationalisierung der vier abhängigen Konzepte eingesetzt wurden, besonders positive Ausprägungen aufweisen. Dabei kann der Implementierungsgrad der Steuerungsmaßnahmen einen Anhaltspunkt zur erfolgreichen Steuerung von Wissensrisiken liefern.

In Tab. 88 sind die Mittelwerte der jeweils 30 Unternehmen mit dem geringsten Erfolg (x(-30)) bzw. mit dem höchsten Erfolg (x(+30)) über die vier abhängigen Konzepte abgetragen. Weiterhin sind die Mittelwerte der gesamten Stichprobe (x (ges.)), die der Top 10 Unternehmen (x(+10)) sowie die der 10 Unternehmen mit den negativsten Ausprägungen (x(-10) über die vier abhängigen Konzepte hinweg berücksichtigt.

	a	**b**	**c**	**d**	**e**	**Δ**	**Δ**	**Δ**
Steuerungsmaßnahme	**x (-10)**	**x (-30)**	**x (ges.)**	**x (+30)**	**x (+10)**	**e-a**	**d-c**	**d-b**
Redundanzschaffung	2,80	3,40	3,90	4,63	5,10	2,3	0,73	1,23*
Wissenstransferrichtlinien	3,10	3,60	4,33	4,80	5,10	2	0,47	1,20
Klassifikation von Wissen	3,50	3,97	4,50	4,93	5,00	1,5	0,43	0,97
Geheimhaltungsvereinbarungen	4,20	4,27	4,77	5,20	5,60	1,4	0,43	0,93
IT-Sicherheitsrichtlinien	4,10	4,30	4,81	5,20	5,70	1,6	0,39	0,90
IT-Sicherheitsbewusstsein	4,10	4,37	4,79	5,10	5,50	1,4	0,31	0,73
Zutrittsbeschränkung	3,60	3,73	4,46	4,33	4,50	0,9	-0,12	0,60
Dynamisierung der Zugriffsrechte	3,70	4,07	4,51	4,63	4,50	0,8	0,12	0,57
Konkurrenzschutzklauseln	3,30	3,17	3,57	3,47	3,70	0,4	-0,10	0,30
Begrenzung der Interaktion	3,20	3,97	4,32	4,17	3,90	0,7	-0,15	0,20
gewerbliche Schutzrechte (IP)	3,30	3,70	3,65	3,70	3,80	0,5	0,05	0,00
Kooperationsvereinbarungen	3,20	3,17	3,36	3,07	2,90	-0,3	-0,30	-0,10
Zugriffsbeschränkung	3,80	4,60	4,42	4,07	3,10	-0,7	-0,35	-0,53

Tab. 88 Steuerungsintensität im Kontext des erfolgreichen Umgangs mit Wissensrisiken

[354] Unternehmen, die in Bezug auf die vier abhängigen Konzepte positive Ausprägungen im Sinne niedriger Wissensrisikopotentiale aufweisen, werden nachfolgend als erfolgreiche Unternehmen bezeichnet. Siehe hierzu auch Abschnitt 7.5.3.

Tab. 88 umfasst verschiedene Mittelwertabweichungen und ist absteigend nach der Mittelwertabweichung zwischen den 30 erfolgreichsten und den 30 Unternehmen mit dem geringsten Erfolg sortiert. Bei einem adjustierten Signifikanzniveau von $\alpha^*=0{,}007$[355] ergibt sich eine signifikante Abweichung in Bezug auf die Maßnahme Redundanzschaffung, die in den Top 30 Unternehmen umfassender implementiert ist. In den Top 10 Unternehmen wird diese Maßnahme nochmals umfassender implementiert, was deren positiven Einfluss zusätzlich unterstreicht. Diese umfassendere Redundanzschaffung dürfte auch ein Grund für die positiven Ausprägungen in Bezug auf die Vertretung, Nachfolge und Reorganisation sein. Dies wurde auch durch zwei Interviewpartner (A, C) bestätigt, die explizit darauf hinwiesen, dass der Verbreitung im Unternehmen eine entscheidende Beutung zukommt und unternehmensintern eine vergleichsweise geringere Begrenzung vorgenommen wird. Dies wurde damit begründet, dass die interne Vertrauensdomäne[356] groß sei und die Weitergabe von Wissen bzw. dessen unternehmensinterne Verbreitung einen kulturellen Wert darstellt. Basierend auf diesen Ergebnissen kann empfohlen werden, die unternehmensinterne Vertrauensdomäne möglichst umfassend zu definieren, um einerseits fluktuationsbedingten Wissensverlusten entgegenzuwirken und andererseits den unternehmensinternen Wissenstransfer zu fördern.

Neben diesen quantitativen Erkenntnissen konnten im Rahmen der vertiefenden Studie qualitative Erkenntnisse gewonnen werden, die zur Fundierung von Handlungsempfehlungen herangezogen werden können. Vergleicht man die 10 erfolgreichsten Unternehmen mit den 10 Unternehmen, die vergleichsweise weniger erfolgreich mit Wissensrisiken umgehen, so ergreifen erstere vergleichsweise umfassender Maßnahmen zur IT-Sicherheit, was auch an einer Mittelwertabweichung von 1,6 deutlich wird. Drei dieser zehn Unternehmen haben mehr als 250 Mitarbeiter, während fünf weitere zwischen 50 und 249 Mitarbeiter beschäftigen. Ein Vertreter eines Großunternehmens (IIIb) und ein Vertreter eines größeren mittelständischen Unternehmens mit 200 Mitarbeitern (IIIa) führten in einem Vertiefungsinterview an, dass ab einer bestimmten Unternehmensgröße eine entsprechend hohe IT-Sicherheit unerlässlich ist, da viele Arbeitsplatzrechner vorhanden sind und daher zur Kontrollierbarkeit rigide und zentral vorgegebene Regelungen essentiell sind. Aus diesem Grund sind für größere mittelständische und insbesondere für Großunternehmen vergleichsweise rigide IT-Sicherheitsrichtlinien zu empfehlen, um so Wissensrisiken, wie z.B. Angriffe auf IT-Systeme oder Zugriffsverletzungen, proaktiv entgegenzuwirken[357]. Auch Geheimhaltungsvereinbarungen werden von erfolgreichen Unternehmen vergleichsweise umfassender implementiert. In den Vertiefungsinterviews wurde die Bedeutung dieser Maßnahme durch zwei der vier befragten Unternehmen (A, D) nochmals betont, wobei ein Ansprechpartner die Geheimhaltung neben rechtlichen Verpflichtungen

[355] Das adjustierte Signifikanzniveau wurde nach Bonferroni-Holm für den Test mit dem niedrigsten p-Wert folgendermaßen errechnet: $\alpha^*= 0{,}1/13=0{,}007$.

[356] Theoretische Überlegungen zur Vertrauensdomäne sind auch von Bedeutung bei der Entwicklung einer IT-Sicherheitsstrategie, die Gegenstand von Abschnitt 4.3 ist.

[357] Für Sicherheitsrichtlinien siehe auch SO1 in Abschnitt 5.10.2.

stark an Maßnahmen zur Sicherstellung der Loyalität knüpfte. Somit sind Maßnahmen zur Sicherstellung der Geheimhaltung durch die Mitarbeiter zu empfehlen (z.B. konkrete Vereinbarungen in Arbeitsverträgen), wobei diese insbesondere auch durch kulturelle Maßnahmen zur Förderung der Loyalität ergänzt werden können. Darüber hinaus ist das IT-Sicherheitsbewusstsein bei den zehn erfolgreichsten Unternehmen vergleichsweise höher, was für eine entsprechende Umsetzung der Sicherheitsmaßnahmen spricht. Ein Ansprechpartner (C) der vier befragten Unternehmen führte an, dass im Unternehmen Maßnahmen zur Schulung und zur Sensibilisierung des sicherheitsbewussten Umgangs mit IT präferiert eingesetzt werden. Aus diesem Grund sind Maßnahmen zur Erhöhung des IT-Sicherheitsbewusstseins zu empfehlen, um Wissensrisiken effizient entgegenzuwirken. So können im konkreten Fall entsprechende Schulungen angeboten werden, um so für potentielle Risiken zu sensibilisieren und Verhaltenserwartungen zu kommunizieren. Letztlich wird auch die Klassifikation von Wissen, die für verschiedene andere Steuerungsmaßnahmen eine Voraussetzung darstellt, vergleichsweise höher durch die zehn erfolgreichsten Unternehmen bewertet, weshalb auch das Ergreifen dieser Maßnahme empfohlen werden kann.

Am geringsten werden im Verhältnis der Teilstichproben in den erfolgreichsten Unternehmen Zugriffsbeschränkungen eingesetzt. Qualitativ kann diese Abweichung nach Angabe von zwei Ansprechpartnern (A, C) der vertiefenden Studie damit begründet werden, dass eine derartige Begrenzung die interne Nutzung und Weiterentwicklung des Wissens hemmen würde. Nach außen hingegen werden vergleichsweise starke Zugriffsbeschränkungen ergriffen. Ein derartiges Vorgehen erfordert nach Aussage eines Ansprechpartners einen vertrauensvollen, loyalen und sicherheitsbewussten Umgang mit Wissen durch die Mitarbeiter. Somit ist anzunehmen, dass eine große interne Vertrauensdomäne und die zugleich starke externe Begrenzung Erfolgsfaktoren in Bezug auf den Umgang mit Wissen darstellen, weshalb ein derartiges Vorgehen empfohlen wird, wobei in diesem Fall unternehmensinterne und -externe Besonderheiten, wie z.B. die Wettbewerbsintensität bzw. das Verhalten der Konkurrenten, zu beachten sind[358].

Neben dem Einsatz der Steuerungsmaßnahmen in den erfolgreichsten Unternehmen wurde in den Unternehmen in der breiten und in der vertiefenden unternehmensinternen Studie die Möglichkeit gegeben, die Steuerungsmaßnahmen anzugeben, denen sie die höchste Bedeutung beimessen. In der breiten Studie wurden die Maßnahmen Dokumentation (16), Personalentwicklung (11), Geheimhaltungsvereinbarungen (10) und Zugriffsbeschränkungen (7) als besonders relevant erachtet[359].

Die Dokumentation von Wissen wurde im Rahmen der Telefoninterviews mehrfach als eine effiziente Maßnahme zur Begrenzung von Wissensverlusten und zur Verbesserung der Zusammenarbeit angeführt. Geheimhaltungsvereinbarungen wurden von sieben (Ia, Ib, IIb, IIIa, IVb, A, D) der 12 An-

[358] Siehe hierzu auch Abschnitt 8.2.4.
[359] Siehe hierzu Abschnitt 7.2.1.

sprechpartner der vertiefenden unternehmensübergreifenden Studie als bedeutende Maßnahme zur Begrenzung der Wissensdiffusion genannt, wodurch deren Potential nochmals hervorgehoben wird und demnach die Ergreifung dieser Maßnahme zu empfehlen ist. Nach Aussage von zwei Ansprechpartnern (A, C) sollten die Zugriffsbeschränkung primär extern ausgerichtet und die interne Vertrauensdomäne möglichst groß gehalten werden, um erwünschte Prozesse nicht zu stark zu hemmen. Da der Umfang der Vertrauensdomäne allerdings stark von der Loyalität und dem Sicherheitsbewusstsein der Mitarbeiter abhängig ist, sind diese Faktoren auch jeweils zu berücksichtigen, weshalb die zu empfehlende Vertrauensdomäne von Unternehmen zu Unternehmen variiert.

Die Priorisierung im Rahmen der vertiefenden unternehmensinternen Studie deckt sich in zwei Fällen mit der breiten unternehmensübergreifenden Studie. So wird den drei Maßnahmen Geheimhaltungsvereinbarungen, Wissenstransferrichtlinien und Zugriffsbeschränkungen das größte Potential zur Risikobegrenzung beigemessen. Während für die beiden erstgenannten Steuerungsmaßnahmen die oben gemachten Aussagen gelten, weisen Wissenstransferrichtlinien ein hohes Steuerungspotential auf, ohne negative Einflüsse auf erwünschte Prozesse zu nehmen. Redundanzschaffung wurde auch von zwei der vier Unternehmen (A, B), die die positivsten Abweichungen über die vier Konzepte aufweisen, als bedeutendste Steuerungsmaßnahme genannt. Insgesamt unterstreichen die Priorisierungen nochmals das Potential der zuvor empfohlenen Steuerungsmaßnahmen.

Als dritte Quelle zur Bestimmung der Potentiale der Steuerungsmaßnahmen kann deren Eignung zur Steuerung mehrerer Wissensrisiken herangezogen werden (siehe Abschnitt 5.11). Maßnahmen, durch die sich bei Unterstellung gleicher Risikoerwartungswerte möglicherweise mehrere Wissensrisiken steuern lassen, können in Bezug auf eine gezielte Allokation von Steuerungsmaßnahmen und der Ergreifung eines Grundschutzes empfohlen werden. Zur Erläuterung dieser Potentiale wurde Tab. 14 auf Seite 240 nochmals aufgegriffen und danach sortiert, wie viele Wissensrisiken durch die Ergreifung der Maßnahmen reduziert werden können.

Steuerungsmaßnahme		**steuerbare Wissensrisiken**	**Σ**
SO5	Richtlinien zur Meldung von Sicherheitsvorfällen	VO6, VO7, VS1, VE1, VE3, VE4, DO1, DO2, DS3, DE1, DE2, DE3, DE7, DE8, DE9	15
SO4	Richtlinien zum Verhalten bei mobiler Arbeit	VP4, VO6, VO7, VE3, VE4, DP1, DO1, DO2, DE7, DE8, DE9	11
SO2	Richtlinien zum Verlassen des Arbeitsplatzes	VP4, VO6, VO7, VE3, DP1, DO1, DO2, DO3, DE7	9
SO13	Verbreitung knapper Kompetenzen	VP1, VP2, VP3, VO1, VE1, VE2, TO3, QP1, QO3	9
SO8	Führung	VP3, VP4, VP5, VE1, DP1, DP2, TP2, TP3	8
SO9	Auswahl der Mitarbeiter	VP4, VP5, DP1, DP2, DE3, TP4, QP3, QO2	8
SO28	vertrauensbildende Maßnahmen	TP1, TP2, TP3, TO4, TO5, TS3, TE2, TE3	8

Tab. 89 Steuerungsmaßnahmen mit Potential zur Steuerung mehrerer Wissensrisiken

In Tab. 89 sind unter Zugrundelegung der literaturbasierten Analyse, die aufgrund des Neuigkeitsgrades des Untersuchungsgegenstandes um Plausibilitätsüberlegungen ergänzt wurde, die acht Maßnah-

men mit dem höchsten Steuerungspotential abgetragen, wobei sich durch deren Ergreifung möglicherweise zwischen 15 und acht Wissensrisiken reduzieren lassen. Darüber hinaus bestehen noch weitere Maßnahmen, durch die sieben oder weniger Wissensrisiken gesteuert werden können. Diese Maßnahmen werden aber an dieser Stelle nicht betrachtet, da in diesem Kontext eine handhabbare Zahl an Steuerungsmaßnahmen betrachtet wird. Durch die Umsetzung von Richtlinien zur Meldung von Sicherheitsvorfällen (SO5) könnten 15 Risiken gesteuert werden. So könnte eine frühzeitige Meldung, das zeitnahe Ergreifen von Steuerungsmaßnahmen und somit eine Begrenzung des Schadensausmaßes ermöglichen. Dadurch könnte beispielsweise der Risikoerwartungswert von Zutritts- und Zugriffsverletzung, von Diebstählen oder Fehlfunktionen reduziert werden. Ebenso könnte der Risikoerwartungswert in 11 Fällen durch die Umsetzung von Richtlinien zur mobilen Arbeit (SO4) reduziert werden, da bedingt durch Fehlverhalten der Mitarbeiter oder die Nutzung vergleichsweise unsicherer Netzwerks- und Kommunikationsverbindungen bei dieser Art der Tätigkeit relativ hohe Risikopotentiale bestehen. Weiterhin könnten Richtlinien zum Verlassen des Arbeitsplatzes (SO2) den Erwartungswert von neun Wissensrisiken reduzieren, da so beispielsweise Zutritts- und Zugriffsverletzungen entgegengewirkt werden kann, indem beim Verlassen des Arbeitsplatzes Büros abgeschlossen bzw. die PCs durch Passwörter geschützt werden. Weiterhin könnten neun Wissensrisiken, die in Zusammenhang mit der Fluktuation stehen, durch die Steuerungsmaßnahme Redundanzschaffung reduziert werden. Dies betrifft beispielsweise Vertretungsverluste, Risiken aus Unternehmenswechsel oder aus Personalausfall. Ferner könnten durch die gezielte Führung der Mitarbeiter acht Wissensrisiken, die primär im Kontext des Wissensverlustes und der -diffusion stehen, begrenzt werden. Dies betrifft beispielsweise eine Reduktion der Eintrittswahrscheinlichkeit von Fehlverhalten oder die Verhinderung der Abwanderung durch verbesserte Mitarbeiterbindung. Darüber hinaus könnten durch die gezielte Auswahl der Mitarbeiter proaktiv acht Wissensrisiken gesteuert werden, wobei insbesondere Risiken im Kontext der mangelnden Qualifikation, potentielles Fehlverhalten oder mangelnde Kompetenzen betroffen sind. Ebenfalls acht Wissensrisiken könnten durch die Ergreifung vertrauensbildender Maßnahmen gesteuert werden. So könnten beispielsweise durch diese Maßnahmen Abwehr- bzw. Vermeidungshaltungen, Zurückhaltung von Wissen oder Risiken eines zu hohen Schutzverhaltens reduziert werden.

Geht man von den theoretischen Überlegungen aus, so könnten bei Unterstellung der Zusammenhänge durch das Ergreifen dieser sieben Steuerungsmaßnahmen 40 der 73 identifizierten Wissensrisiken begrenzt werden. Unterstellt man gleiche Erwartungswerte der Wissensrisiken, so ist das Ergreifen dieser Maßnahmen zu empfehlen, da so durch die Implementierung vergleichsweise weniger Steuerungsmaßnahmen relativ viele Wissensrisiken reduziert werden könnten und folglich eine effiziente Allokation der Steuerungsmaßnahmen vorgenommen werden könnte. In diesem Kontext sind allerdings unternehmensindividuelle Besonderheiten in Bezug auf Relevanz und Stärke der Risikoausprä-

gung ebenso wie empirisch fundierte Vernetzungen der Wissensrisiken und Steuerungsmaßnahmen, die zum aktuellen Zeitpunkt noch nicht bestehen, zu beachten, weshalb keine verallgemeinerbare Empfehlung möglich ist. Vielmehr soll aufgezeigt werden, wie eine gezielte Allokation der Steuerungsmaßnahmen vorgenommen werden könnte.

8.2.2 Steuerungsbedarf von Wissensrisiken

Nachdem das Potential der verschiedenen Steuerungsmaßnahmen näher betrachtet wurde, wird im Rahmen dieses Abschnitts analysiert, welchen Wissensrisiken bei der Steuerung besondere Aufmerksamkeit gewidmet werden sollte. Dazu werden nachfolgend die Risikoerwartungswerte der Einzelrisiken, die Risikoeinschätzungen in der empirischen Studie sowie die Mehrfachsteuerbarkeit der Wissensrisiken herangezogen. Als erste Möglichkeit kann der Steuerungsbedarf durch die Ermittlung der Risikoerwartungswerte identifiziert werden. Im konkreten Einzelfall ergibt sich der primäre Steuerungsbedarf von Wissensrisiken aus der Relevanz und den Risikoerwartungswerten der Einzelrisiken, wobei die Wissensrisiken mit dem höchsten Erwartungswert bevorzugt gesteuert werden sollten.

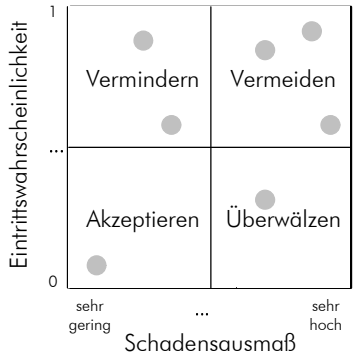


Abb. 43 Erwartungswertmatrix

Legt man nochmals die in Abschnitt 3.5.3[360] erörterte Erwartungswertmatrix (Abb. 43) zugrunde, so ist den Wissensrisiken, die in den Quadranten rechts oben eingeordnet sind, die höchste Priorität in Bezug auf den Steuerungsbedarf zuzuweisen. Bei gleichen Erwartungswerten können zu einer weiteren Priorisierung die Interaktionen zwischen den Wissensrisiken herangezogen werden. Aus der Literatur identifizierte Interaktionen wurden bereits exemplarisch in den Abschnitten 5.3-5.7 dargestellt. Dabei dürften innerhalb der negativ operationalisierten Konzepte Wissensverlust und -diffusion vergleichsweise mehr Interaktionen auftreten, was insbesondere auch durch die erhöhte Anzahl involvierter Akteure zu erklären ist. Über diese Interaktionen hinaus dürften weitere bestehen, die sich bei einer systematischen Auseinandersetzung in der Praxis ergeben könnten. Zum aktuellen Stand der Forschung ist dies jedoch nicht gegeben, wobei in Analogie zum traditionellen bzw. operationellen RM die Steuerung stark interagierender Wissensrisiken bei gleichen Erwartungswerten den Vorteil hätte, eine vergleichsweise stärkere Begrenzung der Gesamtrisikoposition zu erzielen. Weiterhin variiert die Einschätzung der in der Studie eingeschlossenen Wissensrisiken. So bestehen Wissensrisiken, die vergleichsweise gering, und solche, die in der Relation hoch eingeschätzt werden. Betrachtet man die Konzepte aggregiert, so nehmen sie folgende Mittelwerte an: Wissensverlust (WV) 3,39, Wissensdiffusion (WD) 2,91, Wissenstransfer (WT) 4,39, Wissensqualität (WQ) 4,85. In Abb. 44 sind diese Mit-

[360] Siehe hierzu Abb. 13 auf Seite 81.

telwerte und die jeweils minimalen und maximalen Mittelwerte der einzelnen Variablen, die dem Konzept zugeordnet sind, abgetragen, um die Spannweite aufzuzeigen.

Rekodiert man die beiden Konzepte Wissensverlust und Wissensdiffusion, so sind hohe Werte ebenso wie bei den beiden anderen Konzepten als niedrige Risikoausprägung und somit als positiv zu interpretieren. Nach Rekodierung nimmt das Konzept Wissensverlust einen Mittelwert von 4,61 an, während der rekodierte Mittelwert in Bezug auf das Konzept Wissensdiffusion 5,09 beträgt. Auf Basis dieser Werte werden in der Relation Risiken im Kontext der Wissensdiffusion mit einem Mittelwert von 5,09 am geringsten eingeschätzt, während Risiken im Kontext des Wissenstransfers mit einem Mittelwert von 4,39 am höchsten eingeschätzt werden, wobei bei einer näheren Analyse deutlich wird, dass im Gesamtzusammenhang die Wissensrisiken in Bezug auf die positiv operationalisierten Konzepte Wissensqualität und Wissenstransfer über alle Variablen hinweg vergleichsweise homogen eingeschätzt werden, was sich in der vergleichsweise geringeren Spannweite zeigt (siehe Abb. 44). Dies kann weiterhin dadurch unterstrichen werden, dass in der vertiefenden unternehmensinternen Studie durch die 66 Mitarbeiter eines Großunternehmens homogene Einschätzungen dieser Konzepte vorgenommen wurden. Die beiden mit negativen Variablen gemessenen Konzepte Wissensverlust und -diffusion weisen eine vergleichsweise höhere Streuung auf. Diejenigen Variablen, die am jeweiligen Ende der Spannweite angesiedelt sind, sind in der Relation zu den anderen Risiken des Konzeptes stärker ausgeprägt, woraus sich ein Handlungsbedarf ergibt, da davon ausgegangen werden kann, dass diese Wissensrisiken vergleichsweise schlecht unterstützt sind (siehe Abb. 44).

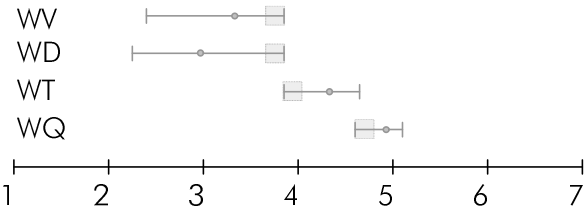


Abb. 44 Spannweite der Konzepte

Unter den Variablen des Konzeptes Wissensverlust werden über alle 129 Unternehmen hinweg die Risiken unzureichende Dokumentation im Tagesgeschäft (3,86), Vertretung (3,81) und Nachbesetzung (3,73) am höchsten eingeschätzt, weshalb in Bezug auf diese Risiken auch der höchste Handlungsbedarf bestehen dürfte. Zur Reduktion des erstgenannten Risikos, das mit Wissensverlusten durch Vergessen einhergeht, könnte auf Basis des in Abschnitt 5.10 entwickelten Maßnahmenkatalogs als mögliche Gegenmaßnahme die Implementierung von Dokumentationsprozessen genannt werden (SO17). Die Dokumentation kann zudem ebenso wie Maßnahmen zur Redundanzschaffung (SO13) und systematische Regelungen zu Nachfolge (SO18) und Vertretung (SO19) den beiden anderen Risiken entgegenwirken.

In Bezug auf die Wissensdiffusion weist Reverse Engineering mit 3,86 den höchsten Mittelwert auf. Neben der Ergreifung der in der Studie eingeschlossenen Maßnahme gewerbliche Schutzrechte können Richtlinien zu Publikationen und Auskünften (SO7), Maßnahmen zur Abwehr von Reverse Engi-

neering (ST7) sowie Vorkehrungen zur Abwehr von Betriebsspionage (SR5) herangezogen werden, um diesem erhöhten Steuerungsbedarf gerecht zu werden. Das Wissensrisiko Reduktion von Abhängigkeiten wird in Bezug auf das Konzept Wissenstransfer mit einem Mittelwert von 3,95 am höchsten eingeschätzt. Die Ergreifung vertrauensbildender Maßnahmen (SO28) könnte zur Reduktion dieses Risikos beitragen, wenn die Potentiale des Wissenstransfers durch den Abbau von Barrieren erhöht würden. Hinsichtlich Wissensqualität wird das Wissensrisiko Anwendbarkeit mit einem Mittelwert von 4,60 am höchsten eingeschätzt. Zur verbesserten Anwendbarkeit dokumentierten Wissens kann dessen Verortung (SO27), die mit einer stärkeren Kontextualisierung einhergeht, als Maßnahme empfohlen werden.

Weiterhin hat die Analyse des Einflusses der Steuerungsmaßnahmen auf die vier abhängigen Konzepte gezeigt[361], dass sich die Wissensrisiken im Hinblick auf die Steuerbarkeit unterscheiden, da eine stärkere Implementierung der 13 Steuerungsmaßnahmen in unterschiedlichem Ausmaß positiv signifikant auf die Risikoausprägung wirkt. Im Hinblick auf die vier abhängigen Konzepte werden insbesondere Wissensrisiken im Bereich Wissensqualität und Wissenstransfer positiv beeinflusst (siehe Tab. 90). In Bezug auf die beiden negativ operationalisierten Konzepte Wissensdiffusion und Wissensverlust liegt eine vergleichsweise schlechtere Steuerbarkeit vor, wobei die Wissensrisiken im Kontext der Nichtdokumentation im Projekt- und Tagesgeschäft sowie der Verlust dokumentierten Wissens durch die intensivere Ergreifung von Steuerungsmaßnahmen reduziert werden könnten. Defizite im Hinblick auf die Steuerbarkeit bestehen somit bei Wissensverlusten aus Vertretung, Nachbesetzung und Reorganisation sowie in Bezug auf alle sechs Wissensrisiken, die dem Konzept Wissensdiffusion zugeordnet sind. Somit sind potentiell weitere als die in der empirischen Studie eingeschlossenen Steuerungsmaßnahmen erforderlich, um diese Wissensrisiken zu begrenzen. Zur Empfehlung von Steuerungsmaßnahmen, die sich potentiell zur Reduktion dieser Risiken eignen, kann die in Abschnitt 5.11 dargestellte plausibilitätsbasierte Vernetzung der Steuerungsmaßnahmen und Wissensrisiken herangezogen werden.

Wissensrisiko	**Konzept**	**Σ (+) EF**
Beitrag externen Wissens	WT	9
Nichtdokumentation (PG)	WV	6
Korrektheit	WQ	6
Rechtzeitigkeit	WQ	5
Nichtdokumentation (TG)	WV	4
Erweiterung der Wissensbasis	WT	4
Reduktion der Abhängigkeit	WT	4
Verfügbarkeit	WQ	4
Aktualität	WQ	4
Qualität externen Wissens	WT	3
Nachvollziehbarkeit	WQ	3
Verlust dokumentierten Wissens	WV	2
Anwendbarkeit	WQ	2
Quantität externen Wissens	WT	1
Nachbesetzung	WV	0
Vertretung	WV	0
Reorganisation	WV	0
unautorisierte Zugriffe	WD	0
nachteilige Mitarbeiterfluktuation	WD	0
Reverse Engineering	WD	0
Imitation	WD	0
Competitive Intelligence	WD	0
unerwünschter Zugang für Partner	WD	0

Tab. 90 signifikante Einflüsse der stärkeren Steuerung

[361] Siehe hierzu Abschnitt 7.3.

Die Risiken, die Wissensverluste aus Nachbesetzung, Vertretung und Reorganisation betreffen, können bei sachlogischer Interpretation durch die Steuerungsmaßnahme Redundanzschaffung reduziert werden. Da die Auswertungen in Abschnitt 7.3 ergeben haben, dass diese Maßnahme keinen signifikant positiven Einfluss auf diese Wissensrisiken nimmt, ist der Einsatz weiterer Maßnahmen zu empfehlen. So könnte in Bezug auf alle drei Wissensrisiken eine umfassende Dokumentation (SO17) einen positiven Beitrag zur Risikoreduktion leisten. Dies wurde auch im Rahmen der vertiefenden unternehmensinternen Studie angeführt (siehe Abschnitt 7.6). Weiterhin können zur Steuerung der beiden erstgenannten Wissensrisiken auch entsprechende Nachfolger- (SO18) bzw. Vertretungsregelungen (SO19) eingesetzt werden.

Auch das Wissensrisiko des unerwünschten Zugangs für Partner lässt sich vergleichsweise schlecht steuern und sollte daher ebenso durch weitere Maßnahmen ergänzt werden. So kann zur Steuerung, wie in Abschnitt 5.11 dargelegt, Kontrolle (SO24) flankierend eingesetzt werden, um die Wahrscheinlichkeit opportunistischen Verhaltens zu reduzieren. Auch die Begrenzung personeller Interaktionspunkte (SO25) kann einen Beitrag zur verbesserten Steuerbarkeit dieses Risikos leisten, da auch so die Kontrollierbarkeit erhöht wird. Aus technischer Sicht kann auch digitales Rechtemanagement (ST10) ergänzend eingesetzt werden, da so eine gezielte Beschränkung der Nutzbarkeit verschiedener Inhalte erfolgen kann. In Bezug auf die in der Studie eingeschlossenen Maßnahmen lässt sich das Risiko der nachteiligen Mitarbeiterfluktuation durch Konkurrenzschutzklauseln steuern. Da diese Maßnahme keinen signifikant positiven Einfluss auf dieses Wissensrisiko nimmt, könnte weiterhin durch gezielte Führung (SO8) die Wahrscheinlichkeit der Abwanderung durch die Identifikation der Mitarbeiterpräferenzen reduziert werden. Zudem könnten Maßnahmen zur Mitarbeiterbindung (SO10), die mit einer Erhöhung des akquisitorischen Potentials einhergehen, zur Risikoreduktion beitragen. Die Bedeutung dieser Maßnahme wurde auch in der unternehmensinternen vertiefenden Studie (siehe Abschnitt 7.6) angeführt. Um Wissensverlusten entgegenzuwirken, kann zudem die Redundanzschaffung (SO13) gefördert werden oder auch die Schaffung bzw. Erhaltung informeller Netzwerke (SO20) angestrebt werden, da so möglicherweise über das Beschäftigungsverhältnis hinausgehend, Wissen noch zur Verfügung steht. Da gewerbliche Schutzrechte als Maßnahme gemäß der Analyse in Abschnitt 7.3 keinen signifikant positiven Einfluss auf die Wissensrisiken Reverse Engineering und Imitation nehmen, können beispielsweise Richtlinien zu Publikationen und Auskünften (S07), die Abwehr von Reverse Engineering (ST7) oder Maßnahmen zur Abwehr von Betriebsspionage (SR5) ergänzend herangezogen werden. Dem Risiko unautorisierter Zugriffe kann eventuell durch eine Variation bestehender Zugriffsrechteprinzipien sowie deren Flankierung durch organisatorische Maßnahmen (z.B. SO1) entgegengewirkt werden.

8.2.3 Austauschbeziehungen beim Einsatz der Steuerungsmaßnahmen

Bei der literaturbasierten Ableitung von Steuerungsmaßnahmen (siehe Abschnitte 5.10.2-5.10.4) und der Konzeption des Interviewleitfadens wurde bereits erörtert, dass Austauschbeziehungen zwischen der Steuerung von Wissensrisiken und der Hemmung erwünschter Prozesse bestehen. Bei der literaturbasierten Analyse des Konzepts konnten insbesondere Interaktionen zwischen den beiden Konzepten Wissenstransfer und Wissensdiffusion identifiziert werden. Besonders evident sind dabei die Zielkonflikte im Kontext der Zusammenarbeit mit Partnern. So ist auf der einen Seite eine intensive Zusammenarbeit erforderlich, um die De- und Rekontextualisierung des Wissens zu erleichtern, wobei auf der anderen Seite mit der Intensität der Zusammenarbeit auch die Potentiale einer unerwünschten Diffusion zunehmen. Weiterhin kann eine umfassende Kontrolle der Zusammenarbeit durch Wissenstransferrichtlinien, Gatekeeper oder Kooperationsvereinbarungen, die darauf ausgerichtet ist, die Risikopotentiale einer unerwünschte Diffusion zu reduzieren, eine Hemmung der Wissenstransferprozesse und somit eine Reduktion der Potentiale und des Erfolgs des Wissenstransfers zur Folge haben (Hamel et al. 1989, 134ff; Lei 1993, 40; Oxley, Sampson 2004, 727). Diese Hemmung ist v.a. auch darauf zurückzuführen, dass die Ergreifung derartiger Maßnahmen als Misstrauen interpretiert werden kann (Norman 2004, 613).

Um diese und weitere Austauschbeziehungen zu evaluieren, wurde in Abschnitt 7.3 eine Analyse des Einflusses der Steuerungsmaßnahmen vorgenommen. Dabei hat sich gezeigt, dass eine umfassendere Implementierung der Steuerungsmaßnahmen in einigen Fällen mit einer negativen Mittelwertabweichung in Bezug auf die Risikoeinschätzung einhergehen kann, allerdings keine dieser Abweichungen zwischen den Teilstichproben signifikant ist. Im Gegenteil stehen die Maßnahmen Wissenstransferrichtlinien und Begrenzung der Interaktion, von denen bei der Konzeption negative Einflüsse auf das Konzept Wissenstransfer erwartet wurden, sogar mit geringeren Wissensrisikoausprägungen in Bezug auf dieses Konzept in Zusamenhang. Dies ist u.a. darauf zurückzuführen, dass klare Regelungen in Bezug auf die Weitergabe von Wissen den Wissenstransfer begünstigen, da Unsicherheiten in Bezug auf die Transferierbarkeit seitens der Mitarbeiter reduziert werden.

Auch wenn auf der Basis der quantitativen Analysen keine Einflüsse identifiziert wurden, so sind die Austauschbeziehungen zwischen der Begrenzung von Wissensrisiken und der Hemmung erwünschter Prozesse auch in den Telefoninterviews der breiten Studie mehrfach thematisiert worden. Aus diesem Grund wurden im Rahmen der vertiefenden unternehmensübergreifenden Studie (siehe Anhang A 2) Austauschbeziehungen erhoben, um qualitative Erkenntnisse zu gewinnen. Eine fallbasierte Erhebung führte zu nachfolgend genannten Austauschbeziehungen.

- **Geheimhaltung vs. Auftragsakquise**: Eine konkrete Austauschbeziehung wurde von den Ansprechpartnern der Unternehmen IIIb und IVb im Kontext des Angebotserstellungsprozesses angeführt. So erfordert dieser Prozess die Offenlegung von sensitiven Inhalten und deren Einbindung

in Konzepte oder Produkte für den Kunden. Erhält das Unternehmen keinen Zuschlag für den Auftrag, so ist das Wissen an den Kunden diffundiert, ohne dass das Unternehmen einen angemessenen Preis dafür erhält.

- **Geheimhaltung vs. effektive Zusammenarbeit**: Weiterhin wurde in drei Fällen (IIa, IVa, D) angeführt, dass eine Austauschbeziehung darin besteht, wie viel Wissen den Partnern offen gelegt wird. So wird die Effektivität der Zusammenarbeit durch den Umfang an offen gelegten Inhalten begünstigt, während dies vielfach mit der Geheimhaltung in Konflikt steht. So ist beispielsweise im Fall von Unternehmen IIa die Offenlegung von Konstruktionsplänen, die eigentlich geheim sind, erforderlich, während in einem anderen Fall (D) Softwarecode offen gelegt werden musste, um eine erfolgreiche Integration der Anwendungen sicherzustellen. Der Ansprechpartner in Unternehmen IVa führte an, dass die Öffnung von IT-Systemen für Partner der Zusammenarbeit förderlich sei, aber mit dem Risiko des Durchgriffs auf sensitive Inhalte einhergeht.
- **Geheimhaltung vs. Sicherung des Vertrauens der Mitarbeiter**: Als eine potentielle Austauschbeziehung wurde vom Ansprechpartner in Unternehmen Ib angeführt, dass Geheimhaltung und Vertrauen der Mitarbeiter zueinander in Wechselwirkung stehen. So wurde ein Problem darin gesehen, dass nur ausgewählte Mitarbeiter über bestimmte sensitive Sachverhalte informiert sind, da dies von nicht informierten Mitarbeitern als Misstrauen ihnen gegenüber interpretiert werden kann und sich daraus negative Auswirkungen auf das Betriebsklima ergeben können.
- **Gewährleistung der Verfügbarkeit vs. Zugriffsbeschränkung**: Der Ansprechpartner in Unternehmen A merkte eine Austauschbeziehung in Bezug auf die Verfügbarkeit dokumentierten Wissens einerseits und der Zugriffsbeschränkung andererseits an. So ist es auf der einen Seite erforderlich, dass Mitarbeiter schnell und möglichst an verschiedenen Orten auf Inhalte zugreifen können. Dies ist aber vielfach aufgrund von Sicherheitsaspekten und den entsprechenden Diffusionsrisiken nicht möglich.

Neben den in der Literatur und den in der empirischen Studie identifizierten Austauschbeziehungen dürfte noch eine Vielzahl weiterer Austauschbeziehungen bestehen, die sich v.a. dann zeigen, wenn der Ansatz des Managements von Wissensrisiken in einem Unternehmen implementiert ist. Somit können die dargelegten Austauschbeziehungen einen ersten Anhaltspunkt liefern und sollen Bewusstsein dafür schaffen, dass die Ergreifung von Maßnahmen zur Reduktion von Wissensrisiken zwar einerseits Risiken steuert, aber andererseits auch negative hemmende Einflüsse haben können, die ihrerseits wiederum Wissensrisiken darstellen.

8.2.4 Einflussfaktoren auf die Risikoausprägung und den Steuerungsbedarf

Im Rahmen der empirischen Studie wurden zwischen den Unternehmen im Hinblick auf die Intensität der Steuerung und die Ausprägungen der abhängigen Konzepte Unterschiede festgestellt. Diese Un-

terschiede können sowohl auf unternehmensinterne als auch auf unternehmensexterne Faktoren zurückgeführt werden. Quantitative Erkenntnisse können dabei aus dem Vergleich der Teilstichproben der jeweils 30 Unternehmen, die in Bezug auf die vier abhängigen Konzepte am erfolgreichsten sind bzw. den geringsten Erfolg aufweisen, gewonnen werden. Weiterhin können qualitative Erkenntnisse aus den 12 Telefoninterviews der unternehmensübergreifenden vertiefenden Studie gewonnen werden. Beide Quellen werden nachfolgend integriert betrachtet und darauf basierend Empfehlungen abgegeben.

Wie in Abschnitt 7.5.3 dargestellt, nehmen eine gesetzliche Verpflichtung zum RM, implementierte RM-Initiativen und WM-Initiativen signifikant positiven Einfluss auf einige Konzepte. So besteht ein signifikant positiver Zusammenhang zwischen einer gesetzlichen Verpflichtung zum RM und der Wissensqualität[362]. Dieser Einfluss kann auf erhöhte Dokumentations- bzw. Nachweispflicht zurückgeführt werden, die mit den entsprechenden Verpflichtungen des RM einhergeht[363]. Dieser Einfluss zeigt sich auch weiterhin darin, dass 50% der Top 30 Unternehmen eine derartige Verpflichtung angeben, während über alle 129 Unternehmen hinweg der Anteil der gesetzlichen Verpflichtung bei 26,36% liegt. Auch die Implementierung von RM-Initiativen steht in einem signifikant positiven Zusammenhang mit der Wissensqualität[364]. Da die gesetzliche Verpflichtung zum RM und das Ergreifen korrespondierender Maßnahmen positiv korrelieren[365], können analog Dokumentations- und Nachweispflichten, die sowohl gesetzlicher als auch freiwilliger Natur sind, als Erklärung angeführt werden. Darüber hinaus korrelieren diese Initiativen positiv mit dem Wissenstransfer[366] und negativ mit dem Konzept Wissensverlust[367], was bedeutet, dass diese Unternehmen Wissensrisiken in beiden Bereichen geringer einschätzen. Dies kann auf das vergleichsweise höhere Risikobewusstsein zurückgeführt werden. Weiterhin ergreifen Unternehmen, die RM-Initiativen implementiert haben, signifikant umfassender Steuerungsmaßnahmen[368]. Im Hinblick auf die Implementierung von RM-Initiativen hebt sich die Teilstichprobe der Top 30 Unternehmen ebenfalls ab. So ergreifen in dieser Stichprobe 66,67% der Unternehmen RM-Maßnahmen, während in Bezug auf alle 129 Unternehmen nur ein Anteil von 52,71% der Unternehmen derartige Initiativen implementiert hat. Aufgrund dieser Zusammenhänge kann zur Reduktion von Wissensrisiken die Implementierung von RM-Initiativen empfohlen werden. Dabei können die Kernaufgaben des Risikomanagements durch eine Vielzahl an Methoden unterstützt werden[369]. Die Implementierung von WM-Initiativen weist analog positive Zusam-

[362] Spearmans Rho beträgt in diesem Fall 0,37, während die Signifikanz bei 0,00002 liegt. Entsprechend der Testmatrix liegt das adjustierte Signifikanzniveau bei $\alpha^*=0,02$.
[363] Siehe hierzu auch Abschnitt 3.6.
[364] Spearmans Rho beträgt in diesem Fall 0,30, während die Signifikanz bei 0,0005 liegt.
[365] Spearmans Rho beträgt in diesem Fall 0,48, während die Signifikanz bei 0,000001 liegt.
[366] Spearmans Rho beträgt in diesem Fall 0,28, während die Signifikanz bei 0,001 liegt.
[367] Spearmans Rho beträgt in diesem Fall 0,28, während die Signifikanz bei 0,001 liegt.
[368] Spearmans Rho beträgt in diesem Fall 0,35, während die Signifikanz bei 0,00005 liegt.
[369] Siehe hierzu auch Abschnitt 3.5.

menhänge wie die Implementierung von RM-Initiativen auf. So bestehen positive Korrelationen mit den positiv operationalisierten Konzepten Wissensqualität[370] und Wissenstransfer[371] sowie eine negative Korrelation mit dem Konzept Wissensverlust[372]. Dies ist möglicherweise auf das erhöhte Bewusstsein für den Wert des Wissens sowie die Förderung der entsprechenden Prozesse zurückzuführen. Weiterhin besteht ein signifikanter Zusammenhang mit der Ergreifung von Steuerungsmaßnahmen[373]. Im Hinblick auf die Implementierung setzen 63,33% der Top 30 Unternehmen WM-Maßnahmen ein, während der Anteil in Bezug auf die Gesamtstichprobe bei 40,31% liegt. Aufgrund des positiven Zusammenhangs kann das Ergreifen von WM-Initiativen empfohlen werden, da dadurch zum einen die Wertschätzung für die Ressource Wissen erhöht werden dürfte und zum anderen signifikant positive Einflüsse auf die Konzepte und die zugrunde liegenden Wissensrisiken bestehen.

Zusätzlich zu diesen quantitativ überprüfbaren Einflussfaktoren, die Gegenstand des Interviewleitfadens sind, werden nachfolgend positive und negative Einflussfaktoren, die in der vertiefenden unternehmensübergreifenden Studie genannt wurden, herangezogen und darauf basierend Empfehlungen abgegeben. Diese Aussagen sind dabei rein qualitativer Natur und sollen einen Eindruck vermitteln, auf welcher Basis positive bzw. negative Ausprägungen über die Konzepte zustande kommen können. In Tab. 91 sind die Einflussfaktoren entsprechend ihrer Nennung in den Vertiefungsinterviews zusammengefasst. Dabei überwiegen die positiven Einflussfaktoren, was dadurch erklärt werden kann, dass neben den acht Unternehmen, die die vier Cluster repräsentieren, auch Vertreter aus den vier Unternehmen, die besonders positive Ausprägungen aufweisen, befragt wurden. Bei einer entsprechenden inversen Betrachtung können auch korrespondierende negative bzw. weitere positive Einflussfaktoren abgeleitet werden. Auf eine derartige Darstellung wird an dieser Stelle allerdings aus Gründen der Übersichtlichkeit und der Dopplung von Einflussfaktoren verzichtet. Die Gruppierung der Faktoren in Tab. 91 erfolgt danach, inwiefern sie in Zusammenhang mit externen Sachverhalten oder internen Ausprägungen stehen. So sind im unternehmensexternen Fall Einflussfaktoren von Relevanz, die in Zusammenhang mit dem Wettbewerb, der Fluktuation, der Art der Zusammenarbeit mit Partnern oder externen Anforderungen seitens des Gesetzgebers stehen. Weiterhin bestehen Maßnahmen bzw. unternehmensinterne Besonderheiten, die eine vergleichsweise stärkere Innenorientierung haben. Dabei können diese Einflussfaktoren in beiden Fällen sowohl unternehmensinterner Natur (i) sein, also von konkreten Maßnahmen bzw. von Besonderheiten des Unternehmens ausgehen, oder in Zusammenhang mit externen Akteuren (e) wie Gesetzgeber, Wettbewerber oder Partnern stehen. Dabei sind auch Mischformen möglich. Dies trifft insbesondere auf Kooperationen zu, da die Zusammenarbeit Handlungen beider Partner erfordert. In Tab. 91 ist darüber hinaus vermerkt, welche der 12 vertiefend

[370] Spearmans Rho beträgt in diesem Fall 0,34, während die Signifikanz bei 0,00007 liegt.
[371] Spearmans Rho beträgt in diesem Fall 0,29, während die Signifikanz bei 0,0008 liegt.
[372] Spearmans Rho beträgt in diesem Fall -0,18, während die Signifikanz bei 0,04 liegt.
[373] Spearmans Rho beträgt in diesem Fall 0,31, während die Signifikanz bei 0,0003 liegt

befragten Unternehmen in den Telefoninterviews die Einflussfaktoren genannt haben. Demnach sind die Abkürzungen Ia/Ib bis IVa/IVb den Vertretern der Cluster und die Abkürzungen A-D den vier Unternehmen, die in Bezug auf die vier abhängigen Konzepte besonders positive Ausprägungen aufweisen, zuzuordnen. Weiterhin sind die zuvor erläuterten RM- und WM-Initiativen in Tab. 91 als Einflussfaktoren abgetragen. Handlungsempfehlungen können dabei primär an den unternehmensinternen Faktoren festgemacht werden, während -externe Faktoren seitens des Unternehmens nicht oder nur in geringem Maße beeinflusst werden können. In Bezug auf das Konzept Wissensverlust beziehen sich die unternehmensübergreifenden Faktoren auf den Wettbewerb bzw. im Speziellen auf die Fluktuation. Somit wird die Wahrscheinlichkeit von Wissensverlusten im Kontext der Interfluktuation von der Zahl der Konkurrenten beeinflusst, da deren Anzahl die Optionen für einen Unternehmenswechsel determiniert und ceteris paribus mit steigender Anzahl das Fluktuationsrisiko steigt (Ib, IIIa).

Faktor	positive Ausprägung	negative Ausprägung

Wissensverlust	**Wettbewerb**
	• (IIIa) wenige Konkurrenten (e)
	• (IIIb/A/C) hohes akquisitorisches Potential (i/e)
	  o z.B. (IIIb) gutes Betriebsklima (i)
	• (IIIa/IIIb/A/B/D) hohe Belegungsstabilität (i)
	  o z.B. (IIIa) vergleichsweise alte Belegschaft (i)
	  o z.B. (IIIb) attraktiver Standort (e)
	• (IIIa) hohe Spezifität der Fähigkeiten (i)
	• (IIIb/A) Übernahme von Auszubildenden (i)
	
	interne Maßnahmen / Besonderheiten
	• (A/C) Dokumentationspflichten (i)
	• (IIIa/IIIb) enge Zusammenarbeit zwischen Mitarbeitern kompensiert Wissensverluste (i)
	• (B) Nachfolgeplanung (i)
	• (quant.) RM-Initiativen (i)
	• (quant.) WM-Initiativen (i)
		Wettbewerb
		• (Ib) viele Konkurrenten (e)
		• (Ia) geringes akquisitorisches Potential (i/e)
		  o z.B. (Ia) geringe Aufstiegschancen (i/e)
		• (Ib) Fachkräftemangel und Wachstumsbranche (e)
		
		interne Maßnahmen / Besonderheiten
		• (Ib) starke Spezialisierung erschwert Vertretung / Nachfolge (i)
		• (Ib) Reorganisation aufgrund Akquisitionen (i)

Wissensdiffusion	**Wettbewerb** • (A) geringe Konkurrenz / kooperativer Wettbewerb (e) • (IVa) Positionierung in einer Nische / wenige Konkurrenten (i/e) • (IVa) geringe externe Zusammenarbeit (i/e) • (C) Reputationsverlust in der Branche bei Fehlverhalten (e) **interne Maßnahmen / Besonderheiten** • (IVb) Management der Zugriffsrechte (i) • (IVa) Limitation der externen Weitergabe (i) • (IVa/D) Definition von Geheimhaltungspflichten (i) • (B) Klassifikation von Wissen und Regelungen zur Weitergabe (i) • (IVa) Konzentration sensitiven Wissens auf Schlüsselmitarbeiter (i) • (D) hohe Spezifität des Wissens (i) • (D) geringe Mitarbeiterzahl (i) • (C) gegenseitige Kontrolle der Mitarbeiter (i)	**Wettbewerb** • (Ia) Konkurrenten kopieren Produkte (e) • (Ia) schwer schützbare Produkte (i) • (Ib) Fluktuation von erfahrenen Mitarbeitern zu Konkurrenten (i/e) **interne Maßnahmen / Besonderheiten** • (Ia/Ib) Begrenzung primär nach außen (i) • (Ia/Ib) offene Unternehmenskultur (i) • (Ia) starke persönliche Bindungen (i) • (Ib) Zusammenarbeit im Bereich der Entwicklung ist mit Partnern unerlässlich (i)

Wissens-transfer	**Art der Zusammenarbeit** • (Ia/A/B/C/D) langjährige Zusammenarbeit (i/e) • (Ia/C) Vertrauen in Partner / Kunden (i/e) • (Ib) starke persönliche Beziehungen (i/e) • (Ib) enger Austausch mit Muttergesellschaft (i) • (Ia) Komplexität der Produkte erfordert intensive Zusammenarbeit (i/e) • (D) vertragliche Absicherung der Zusammenarbeit (i) **interne Maßnahmen / Besonderheiten** • (A/C) Wissenstransfer als Wert im Unternehmen (i) • (A) Weiterbildung von Mitarbeitern für Mitarbeiter (i) • (quant.) RM-Initiativen (i) • (quant.) WM-Initiativen (i)	**Art der Zusammenarbeit** • (IIa / IIb) untergeordnete Rolle von Kooperationen (i)
Wissens-qualität	**externe Anforderungen** • (Ib/quant.) gesetzliche Verpflichtung zum RM / Haftungsrisiken (e) **interne Maßnahmen / Besonderheiten** • (Ia) hohe Qualität der Dokumentationen ist erforderlich für Innovationen in der Entwicklungsabteilung (i) • (A/B) Einsatz von Qualitätsmanagementinitiativen / -systemen (i) • (A/C) hoher Stellenwert der Dokumentation (i) • (C) kurze Halbwertszeit (→ Aktualisierung) (i) • (C) Kundenanforderungen (→ Überprüfung der Korrektheit) (i) • (D) strikte Organisation der Inhalte (i) • (quant.) RM-Initiativen (i) • (quant.) WM-Initiativen (i)	**interne Maßnahmen / Besonderheiten** • (IIa) veraltete IT-Systeme reduzieren Medienqualität (z.B. Bereitstellung, Zugreifbarkeit) (i) • (IIb) standardisierte Prozesse erfordern nur geringe Dokumentation von Wissen (i)

Tab. 91 Einflussfaktoren auf die abhängigen Konzepte

Dieses wird weiterhin durch das akquisitorische Potential (Ia, IIIb, A, C) des Unternehmens (z.B. Vergütung, Sozialleistungen) in der Relation zu Konkurrenten beeinflusst. Im Speziellen wurde durch die Ansprechpartner als Risiko senkender Einflussfaktor ein gutes Betriebsklima genannt (IIIb), während geringe Aufstiegschancen (Ia) einen Risiko erhöhenden Einflussfaktor darstellen. Aufgrund des positiven Einflusses eines hohen akquisitorischen Potentials auf die Wissensrisikopotentiale kann dessen Erhöhung empfohlen werden. Im Konkreten können die Karriereplanung, Vergütung, Anreizsysteme etc. angepasst werden, um so insbesondere fluktuationsbedingten Wissensrisiken proaktiv entgegenzuwirken[374]. Darüber hinaus bestehen spezifische Charakteristika der Belegschaft, die die Fluktuation beeinflussen (IIIa, IIIb, A, B, D). Als Beispiele können zum einen ein vergleichsweise hohes Durchschnittsalter angeführt werden, das die Wechselwahrscheinlichkeit reduziert (IIIa). Zum anderen können auch eine hohe Standortattraktivität bzw. eine Verwurzelung der Mitarbeiter in der Region

[374] Siehe hierzu auch die Anmerkungen zur Steuerungsmaßnahme Mitarbeiterbindung (SO10) in Abschnitt 5.10.2.

angeführt werden (IIIb). Um auf die Belegungsstabilität Einfluss zu nehmen und somit die Fluktuation zu senken, können seitens des Unternehmens neben der Erhöhung des akquisitorischen Potentials auch Investitionen getätigt werden, die zur Erhöhung der Standortattraktivität[375] beitragen. Weiterhin nimmt nach Aussage eines Ansprechpartners (Ib) das Risiko der Interfluktuation zu, wenn ein Fachkräftemangel vorliegt, wobei dieses Risiko nochmals ansteigt, wenn es sich um eine Wachstumsbranche handelt, da dies den Bedarf und die Zahlungsbereitschaft zur Rekrutierung der Mitarbeiter zusätzlich erhöht. In derartigen Fällen ist zur Reduktion der Wirkung dieses Einflussfaktors die eine entsprechende Anpassung der Ausbildungsprogramme und der Personalentwicklung[376] zu empfehlen. Darüber hinaus dürfte das Risiko der Interfluktuation abnehmen, wenn die Fähigkeiten der Mitarbeiter stark unternehmensspezifisch sind (IIIa) und somit deren Einsatz in anderen Unternehmen vergleichsweise schwerer ist. Nach Einschätzung von zwei Ansprechpartnern (IIIb, A) dürfte auch die Übernahme von Auszubildenden Wissensverlusten entgegenwirken, da Humankapital im Unternehmen gehalten wird. Folglich ist deren Übernahme zu empfehlen, um Wissensverluste zu reduzieren und darüber hinaus auch das Risiko der Wissensdiffusion zu Konkurrenten im Kontext der Interfluktuation zu senken.

Hinsichtlich der internen Maßnahmen bzw. Besonderheiten wirken nach Aussage der Ansprechpartner (A, C) Dokumentationspflichten Wissensverlusten entgegen, weshalb sie in die entsprechenden Prozesse integriert werden sollten. Weiterhin kann eine intensive Zusammenarbeit unter den Mitarbeitern (IIIa, IIIb) Wissensverlusten entgegenwirken, die sich aus verschiedenen Formen der Fluktuation ergeben, da dadurch eine stärkere Verbreitung von Wissen und somit eine vergleichsweise einfachere Kompensation von Wissensverlusten erfolgt. Aus diesem Grund sollte die Zusammenarbeit gefördert werden. Dies kann beispielsweise durch eine entsprechende Projektorganisation oder Job Rotation gefördert werden. Darüber hinaus senken nach Aussage eines Ansprechpartners (B) implementierte Nachfolgeregelungen das Risiko von Wissensverlusten, während im umgekehrten Fall eine starke Spezialisierung der Mitarbeiter (Ib) die Risiken aus Nachfolge und Vertretung erhöhen dürfte. Folglich ist die Implementierung entsprechender Nachfolgeregelungen zu empfehlen, um so fluktuationsbedingten Wissensverlusten proaktiv entgegenzuwirken. Als weiterer negativer Risiko erhöhender Einflussfaktor wurden von einem Ansprechpartner (Ib) Reorganisationen, die im Zuge von Akquisitionen durchgeführt wurden, genannt, weshalb bei der Ergreifung derartiger Maßnahmen potentielle Wissensverluste bedacht und eventuell bei der Durchführung der Reorganisation berücksichtigt werden sollten. Aus quantitativer Sicht nehmen implementierte Initiativen zu RM und WM signifikant positiven Einfluss auf das Gesamtkonzept, weshalb sie, wie zuvor erläutert, zur Reduktion von Wissensverlusten implementiert werden sollten.

[375] Als Beispiele können Investitionen in kulturelle Einrichtungen wie z.B. Theater angeführt werden.
[376] Für Details zur Personalentwicklung siehe SO12 in Abschnitt 5.10.2.

Hinsichtlich der unternehmensübergreifenden Zusammenhänge im Kontext der Wissensdiffusion wird deren Risikoerwartungswert zum einen durch eine geringe Anzahl an Konkurrenten (A) oder auch die Positionierung des Unternehmens in einer Marktnische (IVa) reduziert. Weiterhin nimmt nach Aussage eines Ansprechpartners (IVa) das Risiko einer unerwünschten Diffusion ab, wenn die Zusammenarbeit mit anderen Unternehmen eingeschränkt wird, da so die Diffusionspotentiale abnehmen.[377] Eine derartige Einschränkung kann in einigen Fällen zielführend sein, wobei zu beachten ist, dass dadurch möglicherweise Potentiale des Wissenstransfers nicht ausgeschöpft werden und so Risiken eingegangen werden. Aus diesem Grund kann das Ergreifen dieser Maßnahme nicht uneingeschränkt empfohlen werden. Auf der anderen Seite nimmt nach Aussage eines Ansprechpartners (Ia) der Risikoerwartungswert einer Wissensdiffusion zu, wenn Konkurrenten versuchen, die Produkte zu imitieren. Dieses Risiko steigt weiterhin an, wenn die Produkte selbst schwer schützbar sind (Ia). Demzufolge sollten Unternehmen im Falle schwer schützbarer Produkte Maßnahmen zur Reduktion des Reverse Engineering (z.B. Erhöhung der Komplexität oder Spezifität) ergreifen[378]. Der Risikoerwartungswert einer Wissensdiffusion kann dadurch ansteigen, dass erfahrene Mitarbeiter zu Konkurrenten abwandern und ihr Wissen anwenden (Ib). Diesem negativen Einfluss kann durch die Erhöhung des akquisitorischen Potentials entgegengewirkt werden[379]. Weiterhin hat nach Aussage eines Ansprechpartners (C) in einigen Branchen[380] Fehlverhalten wie Eigenangebot sensitiver Inhalte Reputationsverluste für den jeweils anbietenden Mitarbeiter zur Folge. Dieser Reputationsdruck senkt nach Aussage eines Ansprechpartners den Risikoerwartungswert derartigen Fehlverhaltens. Unternehmen können folglich zur Reduktion von Wissensrisiken der Diffusion versuchen, einen derartigen Reputationsdruck in der Branche zu erhöhen, indem sie Fehlverhalten wie die Weitergabe sensitiver Inhalte in der Branche publik machen.

Im Hinblick auf die unternehmensinternen Maßnahmen bzw. Besonderheiten lassen sich Wissensrisiken im Kontext der Wissensdiffusion durch das Management der Zugriffsrechte (IVb) und die Limitation der externen Weitergabe von Wissen (IVa) z.B. im Rahmen von Artikeln oder Informationsmaterialien begrenzen. Derartige Begrenzungen sind zu empfehlen, wobei im Falle von Zugriffsbeschränkungen beachtet werden sollte, dass dadurch die interne Verbreitung von Wissen gehemmt werden kann. Als negative Einflussfaktoren auf die zusammenarbeitsbedingte Wissensdiffusion können dabei eine primär externe Begrenzung (Ia, Ib), eine offene Unternehmenskultur (Ia, Ib) sowie starke persönliche Beziehungen (Ia) zwischen den Mitarbeitern gesehen werden. Somit werden auch bei der Zugriffsbeschränkung die in Abschnitt 5.7 dargelegten Austauschbeziehungen sichtbar. Weiterhin

[377] So nannte ein Ansprechpartner in diesem Fall, dass er sich nicht in Branchenverbänden organisiert.

[378] Siehe hierzu auch die Anmerkungen zur Steuerungsmaßnahme Begrenzung des Reverse Engineering ST7 in Abschnitt 5.10.3.

[379] Siehe hierzu auch die Anmerkungen zur Steuerungsmaßnahme Mitarbeiterbindung (SO10) in Abschnitt 5.10.2.

[380] Das betroffene Unternehmen ist dem Wirtschaftsabschnitt K zugeordnet und bietet spezialisierte Beratungsangebote an.

kann in manchen Fällen die zusammenarbeitsbedingte Wissensdiffusion nur in geringem Maße begrenzt werden. Dies wurde in einem konkreten Fall (Ib) mit der Zusammenarbeit zwischen der Entwicklungsabteilung und Partnern begründet. Diese Offenheit bzw. Vernetzung, die förderlich für den Wissenstransfer ist, weist allerdings ein vergleichsweise geringeres Risikopotential auf, wenn eine entsprechend große Vertrauensdomäne und entsprechende Loyalität der Mitarbeiter bzw. Partner besteht. Aus diesem Grund ist zu empfehlen, Maßnahmen zu ergreifen, die die Loyalität der Mitarbeiter fördern. Neben einer gezielten Beeinflussung der Unternehmenskultur kann auch durch eine entsprechende Führung der Mitarbeiter Einfluss genommen werden. Weiterhin dürften auch die Definition von Geheimhaltungspflichten (IVa, D) sowie klare Regelungen zur Weitergabe von Wissen, die auf einer Klassifikation von Wissen (B) basieren, den Risikoerwartungswert einer Wissensdiffusion reduzieren, weshalb diese Maßnahme zu empfehlen ist. Diese Maßnahmen sind insbesondere auch dann wichtig, wenn vergleichsweise weniger Begrenzungen des Zugriffs und des Zutritts implementiert sind. Eine Begrenzung der Risikopotentiale im Kontext der Wissensdiffusion ergibt sich nach Aussage eines Ansprechpartners (IVa), wenn das sensitive Wissen auf wenige Schlüsselmitarbeiter konzentriert ist. Eine derartige Konzentration kann allerdings nicht uneingeschränkt empfohlen werden, da dadurch die Verfügbarkeit dieser Kompetenzen reduziert werden kann und Wissensverluste in Bezug auf diese Mitarbeiter ein vergleichsweise hohes Schadenspotential aufweisen können. Auch eine hohe Spezifität des Wissens (D) kann eine Erklärung für eine geringe Ausprägung der Wissensdiffusion darstellen, da die Anwendbarkeit durch Dritte erschwert wird. Folglich kann versucht werden, die Spezifität von Wissen in bestimmten Bereichen hoch zu halten[381]. Dies betrifft im Speziellen auch Fähigkeiten der Mitarbeiter, über die potentiell Wissen diffundiert. Darüber hinaus wirkt sich nach Aussage eines Ansprechpartners (D) als Einflussfaktor auch eine geringe Mitarbeiterzahl positiv aus, da die Kontrollierbarkeit der Wissensdiffusion erleichtert wird. Im Falle eines anderen Unternehmens (C) senkt darüber hinaus die gegenseitige Kontrolle der Mitarbeiter die Risikopotentiale der Wissensdiffusion, da die Wahrscheinlichkeit von Fehlverhalten reduziert wird. Eine derartige Kontrolle könnte durch die Schaffung eines entsprechenden Wertes in der Unternehmenskultur implementiert werden. Andererseits können auch formale Kontrollen, wie z.B. das Vier-Augen-Prinzip,[382] in die entsprechenden Prozesse integriert werden.

Im Hinblick auf das Konzept Wissenstransfer betreffen die externen Einflussfaktoren die Art der Zusammenarbeit mit Partnern. Dabei kann eine negative Beeinflussung des Konzeptes darauf zurückgeführt werden, dass Kooperationen eine untergeordnete Rolle für das Unternehmen einnehmen (IIa, IIb). Als positive Einflussfaktoren in Bezug auf den Erfolg des Wissenstransfers wurde von fünf Ansprechpartnern (Ia, A, B, C, D) eine langjährige Zusammenarbeit sowie Vertrauen zwischen den Part-

[381] So können beispielsweise Verfahrensanweisungen eine starke Unternehmensspezifität aufweisen, um so die Anwendbarkeit in einem anderen Unternehmen zu erschweren.

[382] Siehe hierzu auch SO15 in Abschnitt 5.10.2.

ner angeführt, weshalb die Ergreifung vertrauensbildender Maßnahmen[383] zu empfehlen ist. Auch Vertrauen in die jeweiligen Partner bzw. Kunden (Ia, C) dürfte einen positiven Einfluss auf den Wissenstransfererfolg nehmen. Eng in diesem Zusammenhang dürften auch starke persönliche Beziehungen (Ib) zwischen den Partnern einen positiven Einfluss nehmen. Diese können durch regelmäßige persönliche Treffen nachhaltig aufgebaut werden. Die Zusammenarbeit wird nach Aussage eines Ansprechpartners (Ia) auch dann erforderlich, wenn die Komplexität der Produkte hoch ist, da das erforderliche Wissen dann vielfach nicht vom Unternehmen allein generiert werden kann. In diesen Fällen dürfte dem Wissenstransfer eine hohe Bedeutung beigemessen werden. Darüber hinaus führte ein Ansprechpartner (D) an, dass der Wissenstransfererfolg im konkreten Fall durch beiderseitige vertragliche Absicherungen positiv beeinflusst wird. Auch die Ergebnisse der empirischen Studie[384] haben gezeigt, dass derartige Vereinbarungen keinen negativen, sondern vielmehr einen positiven signifikanten Einfluss auf das Konzept Wissenstransfer nehmen, weshalb das Ergreifen dieser Steuerungsmaßnahme empfohlen werden kann. In einem weiteren Fall (Ib) wurden die positiven Ausprägungen in Bezug auf den Wissenstransfer auf einen engen Austausch mit der Muttergesellschaft zurückgeführt. Bezogen auf die internen Maßnahmen bzw. Besonderheiten führten zwei Ansprechpartner (A, C) als Gründe für die vergleichsweise positiven Ausprägungen des Wissenstransfers an, dass der Wissenstransfer einen Wert im Unternehmen darstellt und weiterhin der Weiterbildung, die von Mitarbeitern für Mitarbeiter durchgeführt wird, eine hohe Bedeutung zukommt (A). Aus diesem Grund kann empfohlen werden, dass seitens des Unternehmens die Weitergabe von Wissen als Wert in der Unternehmenskultur verankert wird. Aus quantitativer Sicht bestehen signifikant positive Zusammenhänge zwischen RM- und WM-Initiativen in Bezug auf den Erfolg des Wissenstransfers.

Im Hinblick auf das Konzept Wissensqualität können nach Aussage eines Ansprechpartners (Ib) gesetzliche Verpflichtungen und die daraus erwachsenden Haftungsrisiken eine Ursache für eine hohe Wissensqualität darstellen. Dieser Zusammenhang wird auch durch eine positive Korrelation der Variablen gesetzliche Verpflichtung mit dem Konzept Wissensqualität gestützt. Weiterhin wurde von einem Ansprechpartner (Ia) angeführt, dass insbesondere im Bereich der Entwicklung eine hohe Wissensqualität bedeutend ist, um Innovationen zu ermöglichen. Je nach Spezifika der Unternehmen weisen die Geschäftsbereiche einen unterschiedlichen Bedarf im Hinblick auf die Wissensqualität auf, die im Falle einer Priorisierung von Maßnahmen zur Verbesserung der Wissensqualität berücksichtigt werden sollten[385]. In zwei anderen Unternehmen (A, C) wurde ein hoher Stellenwert der Dokumenta-

[383] Siehe hierzu auch SO28 in Abschnitt 5.10.2.
[384] Siehe für weitere Details Abschnitt 7.3.
[385] So dürfte je nach Ausrichtung und Tätigkeitsschwerpunkt des Unternehmens der Wissensqualität in den jeweiligen Geschäftsbereichen ein unterschiedlicher Stellenwert zukommen. So ist beispielsweise die Wissensqualität in Beratungsunternehmen insbesondere bedeutend, wenn es um die Erstellung von Konzepten und Lösungen für Kunden geht, während in einem Industrieunternehmen die Bedeutung der Wissensqualität in der Produktentwicklung oder in der Qualitätssicherung hoch sein dürfte.

tion angeführt. Darüber hinaus dürften auch bereits implementierte Qualitätsmanagementsysteme bzw. -initiativen eine Erklärung für positive Ausprägungen des Konzeptes darstellen (A, B), da diese zur Verbreitung eines Qualitätsbewusstseins beitragen und somit von einer Ausstrahlungswirkung ausgegangen werden kann. Aufgrund dieser Ausstrahlungswirkung auf das Management von Wissensrisiken kann auch die Implementierung von Initiativen zum Qualitätsmanagement empfohlen werden. Ein weiterer Ansprechpartner (C) führte an, dass eine laufende Aktualisierung dokumentierten Wissens aufgrund dessen kurzer Halbwertszeit unerlässlich ist. Weiterhin wirken sich hohe Qualitätsanforderungen der Kunden (C) positiv auf die Gewährleistung der Korrektheit und somit auf die Wissensqualität aus. Als weiteren Faktor zur Erklärung der positiven Ausprägungen der Wissensqualität führte ein Ansprechpartner (D) an, dass das dokumentierte Wissen strikt organisiert ist und die Mitarbeiter, die dieses Wissen nutzen, ein gemeinsames Verständnis teilen. Folglich sollten ein gemeinsames Verständnis und eine strikte sowie logische Strukturierung der Dokumentenablagen gefördert werden[386]. Im Hinblick auf die ermittelten Korrelationen nehmen neben gesetzlichen Verpflichtungen zum RM auch implementierte RM- und WM-Initiativen einen positiven Einfluss auf die Wissensqualität. Als Erklärung für eine vergleichsweise geringere Ausprägung der Wissensqualität führte je ein Ansprechpartner als Erklärung an, dass die IT-Systeme veraltet (IIa) sind oder aufgrund der Art der Tätigkeiten sowie der Standardisierung der Prozesse (IIb) die Dokumentation von Wissen einen vergleichsweise geringeren Stellenwert aufweist.

Zusammenfassend kann festgehalten werden, dass aufgrund des qualitativen Charakters sowie der geringen Stichprobe diese Ergebnisse zwar erste Anhaltspunkte für Unternehmen, die sich mit dem Management von Wissensrisiken auseinandersetzen, darstellen, aber keine Repräsentativität aufweisen und die Zusammenhänge vielmehr hypothetischer Natur sind, weshalb sie in nachfolgender Forschung einer empirischen Validierung bedürfen.

8.2.5 Integrierte Betrachtung und Diskussion

Aufgrund der Heterogenität von Unternehmen und der Vielzahl an bestehenden internen und externen Einflussfaktoren können bei der Steuerung von Wissensrisiken nur wenige allgemeingültige Empfehlungen abgegeben werden. Vielmehr ist eine Einzelfallbetrachtung erforderlich. Aus diesem Grund wird nachfolgend erörtert, wie beim Management von Wissensrisiken vorgegangen werden kann und wie die gewonnenen Erkenntnisse in diesen Prozess gewinnbringend einfließen können. Den Kern dieses Vorgehens bildet der Wissensrisikomanagementprozess, dessen Phasen jeweils unterstützt werden können. Die relevanten Erkenntnisse werden nachfolgend ausgehend von der Identifikation wissensbezogener Ressourcen über die weiteren Prozessphasen hinweg erörtert, wobei Abb. 45 zur Strukturierung dieser Erkenntnisse dient.

[386] Siehe hierzu auch die Ausführungen in der vertiefenden unternehmensinternen Studie Abschnitt 7.6.6.

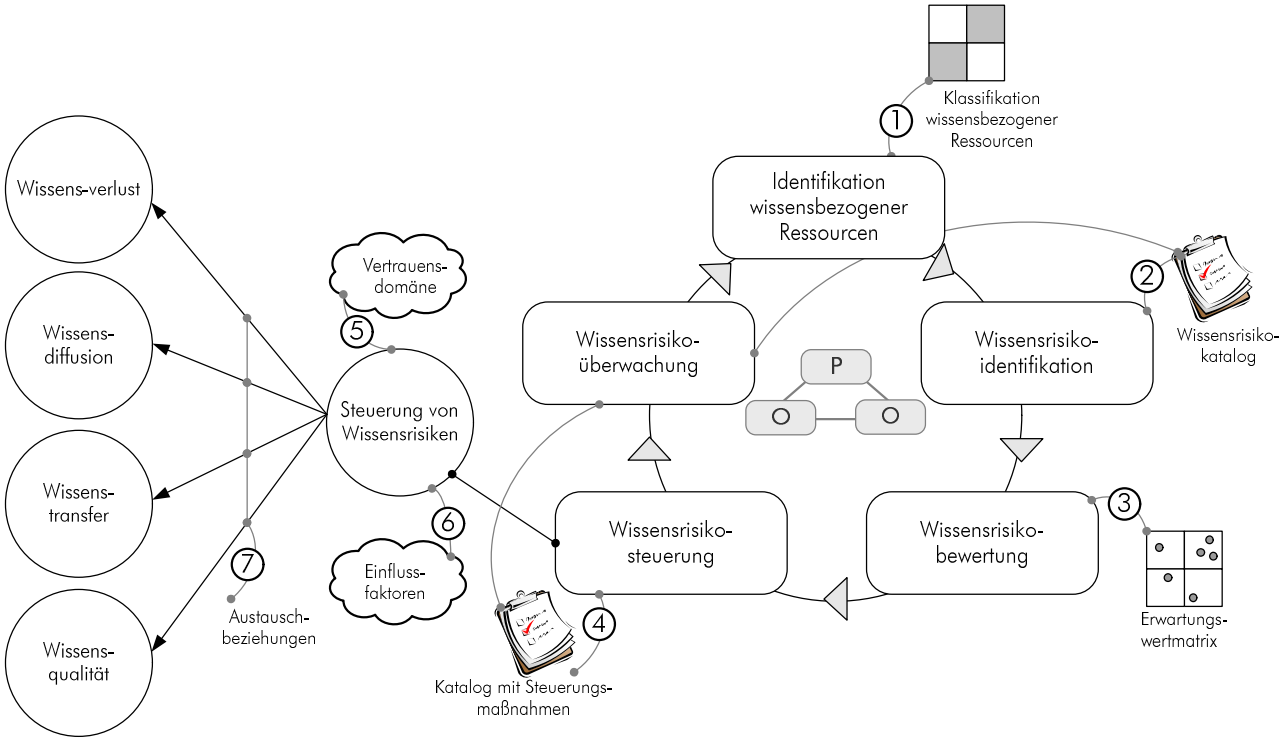


Abb. 45 Unterstützung der Steuerung von Wissensrisiken

(1) **Konzentration auf zu schützende wissensbezogene Ressourcen**: Da es aus ökonomischen Gründen nicht tragfähig ist, alle wissensbezogenen Ressourcen, über die ein Unternehmen verfügt, beim Management von Wissensrisiken zu berücksichtigen, sollte eine Priorisierung der wissensbezogenen Ressourcen entsprechend ihres Schutzbedarfes vorgenommen werden. Demnach sollten Unternehmen auf diejenigen Ressourcen abstellen, die eine hohe Werthaltigkeit aufweisen und die Steuerungsmaßnahmen gezielt auf diese Ressourcen allokieren. In Bezug auf die in Abschnitt 8.1 entwickelte Heuristik zur Klassifikation (siehe Abb. 42) sind v.a. wissensbezogene Ressourcen, die dem Quadranten I zugeordnet sind, betroffen.

(2) **Nutzung des Wissensrisikokataloges**: Die Identifikation von Wissensrisiken kann durch die Nutzung des literaturbasiert abgeleiteten Wissensrisikokataloges gestützt werden. Dieser kann die Analyse entlang der Geschäftsprozesse oder Geschäftsbereiche unterstützen[387]. Neben der Identifikation von Wissensrisiken ist dieser Katalog auch für die Wissensrisikoüberwachung von Relevanz, da so nach Durchlaufen des Wissensrisikoprozesses zu den Wissensrisiken Indikatoren zur Überwachung definiert werden können[388]. Die Nutzung dieses Katalogs kann eine erste Unterstützung bei der Identifikation der Wissensrisiken geben, wobei zu beachten ist, dass ein Einsatz in Unternehmen erforderlich ist, um die Praktikabilität einzuschätzen und eine empirische Validie-

[387] Siehe hierzu auch die Abschnitte 3.5.2 und 5.9.2.
[388] Siehe hierzu auch die Anmerkungen in den Abschnitten 3.5.5 und 5.9.5.

rung vorzunehmen. Durch diesen Einsatz könnte eine Konsoldierung und Erweiterung des Katalogs erreicht werden.

(3) **Priorisierung der Wissensrisiken auf Basis der Erwartungswertmatrix**: Unternehmen unterschieden sich darin, wie relevant die in den Abschnitten 5.3-5.6 dargestellten Wissensrisiken sind und welche konkreten Eintrittswahrscheinlichkeiten bzw. Schadensausmaße diesen Risiken beigemessen werden können. Dies haben auch die unternehmensinterne (siehe Abschnitt 7.6) und die unternehmensübergreifende vertiefende Studie (siehe Abschnitt 7.5) gezeigt. Zur Ermittlung von Eintrittswahrscheinlichkeiten und Schadensausmaßen zur Bildung von Risikoerwartungswerten können im Rahmen der Wissensrisikobewertung die in Abschnitt 5.9.3[389] dargestellten Quellen genutzt werden. Die resultierenden Erwartungswerte sollten in einer entsprechenden Matrix abgetragen werden, um zu determinieren, welche Wissensrisiken primär gesteuert werden sollen. Der Steuerungsbedarf ergibt sich dann aus der jeweiligen Risikoneigung des Unternehmens.

(4) **Nutzung des Katalogs an Steuerungsmaßnahmen**: Die Steuerung von Wissensrisiken kann durch den in den Abschnitten 5.10.2-5.10.4 entwickelten Katalog unterstützt werden. Neben der Steuerung ist dieser Katalog auch für die Wissensrisikoüberwachung von Relevanz, da im Rahmen dieser Aufgabe die Eignung und Effizienz der eingesetzten Steuerungsmaßnahmen überprüft wird und Anpassungen des Katalogs eine Folge sein können. Dabei ist allerdings zu beachten, dass die Vernetzung der Steuerungsmaßnahmen und Wissensrisiken aufgrund des Neuigkeitsgrades des Themengebiets primär auf Plausibilitätsüberlegungen basiert und somit eine empirische Fundierung erforderlich ist. Dennoch kann die Darlegung der verschiedenen Steuerungsmaßnahmen einen Beitrag leisten, wobei die in der empirischen Studie einbezogenen Maßnahmen hinsichtlich ihrer Wirksamkeit bereits analysiert wurden. Darüber hinaus wurden seitens der Interviewpartner im Rahmen der empirischen Studie auch Varianten an Steuerungsmaßnahmen genannt (siehe 7.7), die werthaltig sein können. Diese Varianten sollten demnach beim Einsatz von Maßnahmen berücksichtigt werden. Weiterhin hat die empirische Studie gezeigt, dass die Risiken sich in Bezug auf ihre Steuerbarkeit unterscheiden. Durch die Ergreifung von Steuerungsmaßnahmen, die sich zugleich zur Reduktion mehrerer Wissensrisiken eignen, kann eine gezielte Allokation der Steuerungsmaßnahmen erreicht werden und die Gesamtrisikoposition erheblich reduziert werden, sofern diese Wissensrisiken hohe Erwartungswerte aufweisen.

(5) **Beachtung der Vertrauensdomäne**: Die vertiefenden Studien (siehe Abschnitte 7.5 und 7.6) haben gezeigt, dass die Intensität der Steuerung von den Charakteristika des Unternehmens abhängt. Die erfolgreichsten Unternehmen stellen dabei v.a. auf eine intensive Redundanzschaffung und zugleich auf eine geringe unternehmensinterne Zugriffsbeschränkung ab. Weiterhin haben die Vertiefungsinterviews gezeigt, dass eine derartige Allokation der Steuerungsmaßnahmen eine ho-

[389] Siehe hierzu auch Anhang A 3.

he Loyalität der Mitarbeiter erfordert. Dabei variiert die Loyalität von Unternehmen zu Unternehmen, wodurch die resultierende Vertrauensdomäne beeinflusst wird.

(6) **Beachtung von Einflussfaktoren**: Die vertiefenden empirischen Studien (siehe Abschnitte 7.5 und 7.6) haben gezeigt, dass der erfolgreiche Umgang mit Wissensrisiken durch unternehmensinterne und -externe Faktoren beeinflusst wird. So kann beispielsweise eine hohe Anzahl an Konkurrenten das Diffusionsrisiko erhöhen, während durch die Positionierung in einer Marktnische diese Risikopotentiale abnehmen. Insgesamt beeinflussen diese Faktoren den Einsatz von Steuerungsmaßnahmen und sind im Einzelfall ebenso wie die Relevanz bestimmter Risiken zu reflektieren.

(7) **Beachtung potentieller Austauschbeziehungen**: Die Literaturanalyse und die vertiefende qualitative Studie haben gezeigt, dass einige Steuerungsmaßnahmen potentiell erwünschte Prozesse hemmen. Bei der Auswahl der Steuerungsmaßnahmen sollten diese Effekte beachtet werden und bei Ergreifung dieser Steuerungsmaßnahmen eine entsprechende Überwachung im Sinne der Kernaufgaben des RM erfolgen. Im umgekehrten Fall können Steuerungsmaßnahmen ohne derartige Austauschbeziehungen vorbehaltlos eingesetzt werden.

Die in dieser Arbeit entwickelten Methoden, die Kataloge an identifizierten Wissensrisiken, Steuerungsmaßnahmen und deren Vernetzung sowie die aus den empirisch gewonnenen Erkenntnisse können zu einer ersten Unterstützung des Managements von Wissensrisiken beitragen und die entsprechenden Kernaufgaben im Wissensrisikomanagementprozess unterstützen (siehe Abb. 45). Weiterhin soll mithilfe des nachfolgenden Abschnitts aufgezeigt werden, wie das Management von Wissensrisiken in Unternehmen implementiert werden kann und welche Ansatzpunkte bestehen.

8.3 Implementierung der Steuerung von Wissensrisiken

Eine effiziente Steuerung von Wissensrisiken bedarf einer organisatorischen Verankerung. Daher sind Handlungsempfehlungen zur Implementierung der Steuerung von Wissensrisiken in der Aufbau- und Ablauforganisation Gegenstand dieses Abschnitts. Zur Fundierung des Implementierungskonzeptes wurden im Rahmen der vertiefenden unternehmensübergreifenden Studie alle 12 Unternehmen zu potentiellen Ansatzpunkten in den beiden Bereichen befragt[390]. Neben den Interviews werden bei den nachfolgenden Betrachtungen auch auf der Literatur basierende Vorschläge zur Implementierung herangezogen. Im Rahmen der Aufbauorganisation wurde von sieben der 12 Interviewpartnern (Ia, Ib, IIa, IIIa, IIIb, IVa, C) der vertiefenden unternehmensübergreifenden Studie als möglicher Ansatzpunkt für die Implementierung der Steuerung von Wissensrisiken die Schaffung einer oder mehrerer Rollen genannt, während die Schaffung einer eigenen Stelle aufgrund der mangelnden Präzision der Aufgabengebiete und aus Kostenaspekten von zwei Ansprechpartnern (IIIa, C) verneint wurde. Als mögliche Aufgabengebiete wurden die Kommunikation der Geheimhaltungsverpflichtungen, Sensibilisierung der Mitarbeiter, Erarbeitung von Schutzkonzepten, Erarbeitung von Wissenstransferrichtlinien, Überprüfung der bestehenden technischen Sicherheitsvorkehrungen auf Tauglichkeit sowie Forcierung der Durchsetzung gewerblicher Schutzrechte genannt.

Da das Aufgabengebiet vergleichsweise breit ist und organisatorische, technische und rechtliche Aspekte gleichermaßen einschließt, wurde in zwei Interviews (IIIb, C) betont, dass es sich im Unternehmen um eine verteilte Rolle handeln sollte. Im Rahmen eines Interviews mit einem Ansprechpartner aus einem Großunternehmen wurden bei einem Einsatz verteilter Rollen die Erfordernisse der Koordination sowie eine gemeinsame Ausrichtung dieser Rollen angemerkt. Während die Koordination nach Aussagen der Interviewpartner durch eine klare Aufgabenabgrenzung erreicht werden kann, sollte die gemeinsame Ausrichtung durch Vorgaben der Geschäftsleitung, die durch regelmäßige Meetings begleitet werden kann, gestützt werden. Basierend auf den Aussagen der Interviewpartner kann die Implementierung von Rollen in der Aufbauorganisation empfohlen werden, wobei die konkrete Ausgestaltung durch die Charakteristika des Unternehmens und dabei insbesondere durch die Unternehmensgröße determiniert wird. Seitens der Interviewpartner wurden verschiedene Aufgabenbereiche dieser Rollen genannt, die auf Basis der Literatur detailliert werden können.

Reflektiert man die unterschiedlichen Aufgabengebiete im Kontext der Steuerung von Wissensrisiken, so lassen sich bereits in Unternehmen existierenden Rollen spezifische Teilaufgaben zuordnen. Im Rahmen der Analyse der Aufgabengebiete des Wissensmanagers (CKO) in 300 Fällen stellte sich nach Asllani und Luthans (2003, 53ff) heraus, dass sich CKOs nur zu einem geringen Anteil mit Sicherheitsaufgaben befassen und primär Aufgaben im Kontext der klassischen Kernprozesse des WM,

[390] Siehe hierzu auch den Fragebogen zur vertiefenden unternehmensübergreifenden Studie in Anhang A 2.

die beispielsweise Identifikation, Erwerb, Entwicklung und Verteilung von Wissen einschließen, wahrnehmen[391]. Ungeachtet dessen sind Kenntnisse in Bezug auf dieses Aufgabenspektrum bzw. diese Prozesse für die Implementierung eines derartigen Konzeptes von Relevanz. So kann insbesondere die Identifikation wissensbezogener Ressourcen sowie die Integration von Aspekten des Wissensrisikomanagements in bestehende WM-Initiativen durch den Wissensmanager verantwortet werden.

Neben dem Wissensmanager könnte auch ein Risikomanager (CRO) einbezogen werden, da so eine Integration des Managements von Wissensrisiken in das bestehende unternehmensweite RM erfolgen könnte. Risikomanager überstehen den operativ verantwortlichen Risikobeauftragten, sind mit den Kernaufgaben des traditionellen RM in strategischer und methodischer Hinsicht betraut und können zudem einschätzen, welche gesetzlichen und regulatorischen Anforderungen an das Unternehmen gerichtet sind[392].

Darüber hinaus ist auch die Rolle des Sicherheitsmanagers von Relevanz, die beispielsweise die Implementierung und Überwachung von Zutrittskontrollen, Brandmeldeanlagen oder Einbruchsmeldeanlagen ausgerichtet ist. Im Kontext der Abwehr von Wirtschaftsspionage wird das Rollenprofil um die Aufgabengebiete Informationsbeschaffung bei Sicherheitsbehörden, Durchführung von Risiko- und Schwachstellenanalysen, Erarbeitung sicherheitsorientierter Arbeitsabläufe, regelmäßige Pflege und Aktualisierung des Sicherheitssystems oder Vorbereitung sicherheitspolitischer Entscheidungen spezifiziert (Dreger 1998, 310f; Verfassungsschutz 2004a, 8f).

Spezifische Aufgaben im Bereich des IT-RM werden dem IT-Sicherheitsmanager zugewiesen. Analog zum Sicherheitsbeauftragten betreffen die Aufgabengebiete dieser Rolle die Implementierung von Sicherheitsmaßnahmen in Bezug auf den Betrieb der IT-Systeme. So umfassen die Aufgaben z.B. die Erstellung von Zugriffskontrollkonzepten, die Erarbeitung von IT-Sicherheitsrichtlinien, das Einspielen von Patches, die Implementierung und Aktualisierung von Firewalls und Virenscannprogrammen sowie die Schulung der Mitarbeiter (BSI 2006, 1409ff).

Im Hinblick auf den unternehmensübergreifenden Wissenstransfer können Rollen geschaffen werden, die Wissenstransferprozesse kontrollieren bzw. den Transfer bestimmten Wissens genehmigen oder verweigern. Derartige Rollen werden in der Literatur vielfach als Gatekeeper oder Kooperationsmanager bezeichnet (Hamel et al. 1989, 136; Fleischer 1997, 238; Loebbecke et al. 1999, 20; Awazu 2004b, 21). In diesem Zusammenhang sprechen sich McGonagle und Vella für die Schaffung einer nicht namentlich spezifizierten Rolle aus, die dafür verantwortlich ist, zu überprüfen, inwiefern die Inhalte, die Externen z.B. im Rahmen von Tagungen, oder Zeitungsinterviews zugänglich gemacht werden sollen, sicherheitskritisch bzw. vertraulich sind (McGonagle, Vella 1994, 294). Diese Anfor-

[391] Siehe hierzu auch (Upadhyaya et al. 2006, 795).

[392] Für eine Übersicht an Rollen im Kontext des RM siehe (Locher et al. 2004, 27f). Für eine philosophische Betrachtung der Rolle des Risikomanagers siehe (Bieta 2002, 17ff).

derungen stellen somit eine Erweiterung der Aufgabengebiete des auf Kooperationen fokussierten Gatekeepers auf sämtliche Prozesse, die über die Grenzen des Unternehmens hinausgehen, dar[393].

Neben den organisatorischen und technischen Aufgaben schließt die Steuerung von Wissensrisiken auch rechtliche Aspekte ein, die sich vorwiegend auf die Ergreifung bzw. Durchsetzung gewerblicher Schutzrechte beziehen. Diese Aufgabengebiete betreffen in der Regel die Rechtsabteilung des Unternehmens und werden im Folgenden unter der Rolle IP-Beauftragter zusammengefasst. Nach Awazu und Desouza[394] ist die Rolle darauf ausgerichtet, die unautorisierte Nutzung, den Diebstahl und die Sabotage sensitiver Inhalte zu verhindern. Als weitere Aufgabengebiete ist der IP-Beauftragte in Patentfragen, Compliance und Steuerung von Kooperationen involviert, wobei letztere die Erstellung entsprechender vertraglicher Regelungen betrifft (Awazu, Desouza 2004, 23f). Im Hinblick auf gewerbliche Schutzrechte wie Patente oder Urheberrechte sind in diesem Zusammenhang die Beantragung und die rechtliche Durchsetzung von Schutzrechtsverletzung relevant.

Rolle	wissensrisikomanagementspezifische Aufgaben
Wissensmanager	• Sensibilisierung für den Wert wissensbezogener Ressourcen • Unterstützung der Identifikation wissensbezogener Ressourcen • Implementierung von WM-Initiativen und Integration von Wissensrisikoaspekten
Risikomanager	• Integration des Wissensrisikomanagements in das unternehmensweite RM • Unterstützung der Kernaufgaben des Wissensrisikomanagements durch Methoden und Verfahren des traditionellen RM
Sicherheitsmanager	• Implementierung und Adaption technischer und organisatorischer Maßnahmen, die bauliche Aspekte betreffen, entsprechend der Anforderungen und Besonderheiten, die sich aus dem Wissensrisikomanagement ergeben
IT-Sicherheitsmanager	• Implementierung und Adaption technischer und organisatorischer Maßnahmen, die die IT-Systeme betreffen, entsprechend der Anforderungen und Besonderheiten, die sich aus dem Wissensrisikomanagement ergeben
IP-Manager	• Implementierung und Adaption rechtlicher Maßnahmen entsprechend der Anforderungen und Besonderheiten, die sich aus dem Wissensrisikomanagement ergeben
Gatekeeper	• Kontrolle des Wissenstransfers entsprechend der Anforderungen und Besonderheiten, die sich aus dem Wissensrisikomanagement ergeben
Qualitätsmanager	• Integration von Aspekten der Wissensqualität in bestehende Qualitätsmanagementinitiativen und -systeme

Tab. 92 Aufgaben der verschiedenen Rollen im Kontext des Wissensrisikomanagements

Darüber hinaus kann auch die Rolle eines Qualitätsmanagers bei der Implementierung des Managements von Wissensrisiken einbezogen werden. Diese Rolle kann dahingehend erweitert werden, dass sie zur Erhöhung der Qualität dokumentierten Wissens beiträgt und das Qualitätsmanagement bzw. das -system entsprechend anpasst[395].

Zusammenfassend ist somit in Bezug auf die Umsetzung der Steuerung von Wissensrisiken in der Aufbauorganisation die Erweiterung der Aufgabengebiete der Rollen Wissensmanager, Risikomana-

[393] Weiterhin könnten speziell zur Verbesserung des interorganisatorischen Wissenstransfers Boundary Spanner als Rollen eingesetzt werden, die die Vernetzung mit externen Partnern fördern (Brown, Duguid 1998, 102ff; Cross, Prusak 2002, 106ff; Awazu 2004a, 63f).

[394] Awazu und Desouza bezeichnen diese stärker rechtlich fokussierte Rolle als Chief Privacy Officer (CPO).

[395] Basierend auf den Erkenntnissen aus den Telefoninterviews erscheint die Einbeziehung dieser Rolle insbesondere für Unternehmen von Relevanz, die im Gesundheitswesen tätig sind.

ger, Sicherheitsmanager, IT-Sicherheitsmanager, IP-Manager, Gatekeeper sowie Qualitätsmanager denkbar bzw. zu empfehlen (siehe Tab. 92 und Abb. 47). Aufgrund der thematischen Nähe sollten die Risiko- und Wissensmanager die fachliche Führung übernehmen. Je nach Charakteristika des Unternehmens können Rollen bzw. Aufgabenverteilungen variieren, wobei die genannten Rollen in diesem Kontext nur mögliche Ansatzpunkte aufzeigen sollen. So ist in diesem Zusammenhang in kleinen und mittelständischen Unternehmen davon auszugehen, dass im Vergleich zu Großunternehmen keine strikte Rollentrennung vorgenommen wird, sondern bedingt durch die geringere Mitarbeiterzahl vielmehr von einer Stelle mehrere Rollen gleichzeitig übernommen werden.

In Bezug auf den Wissensrisikomanagementprozess könnten diese Rollen vorwiegend damit betraut werden, Steuerungsmaßnahmen entsprechend ihres Aufgabenschwerpunktes zu erarbeiten und in Abhängigkeit der Effizienz der Risikobewältigung diese Maßnahmen anzupassen bzw. neue adäquate Maßnahmen zu entwickeln. Der Wissensmanager sollte aufgrund seiner Fokussierung auf die Wissensprozesse des Unternehmens die Identifikation der wissensbezogenen Ressourcen unterstützen.

Neben der Schaffung von organisatorischen Rollen, die die Implementierung der Steuerung von Wissensrisiken unterstützen, ist auch eine Integration der Wissensrisikoaspekte in die jeweiligen operativen Prozesse des Unternehmens zu empfehlen, um über alle Unternehmensebenen hinweg eine effiziente Steuerung sicherzustellen (siehe Abb. 47). Nach Aussage von acht der 12 Interviewpartner (Ia, Ib, IIa, IIIa, IIIb, IVa, IVb, C) der vertiefenden Studie ist eine Implementierung auf der Ebene der Geschäftsprozesse sinnvoll und vorstellbar, da so eine Integration in die täglichen Abläufe der operativ verantwortlichen Mitarbeiter gewährleistet werden könnte. Als mögliche Ansatzpunkte wurde durch zwei Unternehmen (Ia, IVa) die Erweiterung des Qualitätsmanagementhandbuches oder die Erweiterung entsprechender Verfahrensanweisungen genannt. Im Falle eines projektorganisierten Unternehmens (C) wurde die Erweiterung des Projektmanagementhandbuches vorgeschlagen, während durch zwei Unternehmen des verarbeitenden Gewerbes (IIIa, IVb) die Integration in Arbeitsanweisungen bzw. Workflows vorgeschlagen wurde[396]. In einem dienstleistungsorientierten Unternehmen, für das dokumentiertes Wissen von besonderer Bedeutung ist, wird in Bezug auf die Implementierung der Steuerung dem Zugriffsrechtekonzept die zentrale Bedeutung beigemessen, um der Austauschbeziehung zwischen Verfügbarkeit und Schutz des dokumentierten Wissens gerecht zu werden. Entsprechend dieser Aussagen bestehen im Wesentlichen zwei generische Ansatzpunkte zur Implementierung der Steuerung auf der operativen Ebene. So können zum einen die Projektmanager und zum anderen die Prozessmanager die Anforderungen an die operativ verantwortlichen Mitarbeiter übersetzen und in entsprechende Verfahrensanweisungen, Prozessbeschreibungen oder Workflows überführen. Die Bestimmung der Prozesse bzw. Projekte mit besonders hohem Schutzbedarf kann durch die Unterneh-

[396] Im Falle eines Kleinstunternehmens wird die Steuerung von Wissensrisiken durch detaillierte Regelungen zu den Arbeitnehmerpflichten in Arbeitsverträge implementiert.

mensleitung als Gremium vorgenommen werden, das je nach Unternehmensgröße, -organisation und -kultur Geschäftsbereichs-, Bereichs-, Abteilungs- und Gruppenleiter einschließen kann. So wurde durch drei Interviewpartner (Ib, IIa, IVb) darauf hingewiesen, dass sowohl die Klassifikation wissensbezogener Ressourcen als auch die Bestimmung, welche Projekte oder Prozesse unter Sicherheitsaspekten besonders kritisch sind, Top Down erfolgen sollte, wobei zwei dieser Ansprechpartner die Definition durch ein Gremium als vorteilhaft anführten, da so einerseits die Basis zur Identifikation relevanter Themen verbreitert wird und andererseits die Kommunikation auf tiefere Managementebenen sichergestellt werden kann. Die vertiefende Studie hat gezeigt, dass anstelle von Prozess- und Projektmanagern im Gesundheitswesen diese Aufgaben durch Qualitätsmanager übernommen werden können[397]. Diese könnten dann die entsprechenden Anforderungen in Verfahrensanweisungen umsetzen. Die Einschätzung, wann ein Prozess oder Projekt aus Wissensrisikoperspektive besonders kritisch ist und somit einen erhöhten Schutzbedarf aufweist, kann sich auf mehrere Kriterien stützen. Dabei sind zum einen die Faktoren, die im Hinblick auf die Klassifikation wissensbezogener Ressourcen herangezogen werden, von Relevanz.

Kriterium	Beschreibung
Wettbewerbsrelevanz	Der Steuerungsbedarf von Projekten und Prozessen nimmt dann zu, wenn diese wettbewerbsrelevant sind und beispielsweise zu Kostenvorteilen oder zur Differenzierung des Unternehmens beitragen. Umso stärker dieser Zusammenhang ist, umso höher ist deren Schutzbedarf, um die Wettbewerbsfähigkeit nachhaltig zu sichern.
Wertschöpfungsbeitrag	Tragen die Prozesse bzw. Projekte vergleichsweise stark zur Erstellung der Wertschöpfung bei, so ist darauf zu achten, dass Wissensrisiken, die die Durchführung hemmen, begrenzt werden. Derartige Wissensrisiken können beispielsweise darin bestehen, dass relevantes Wissen stark auf einzelne Mitarbeiter konzentriert ist und somit potentielle Engpässe entstehen. Aufgrund des Wertschöpfungsbeitrags der Prozesse bzw. Projekte sollte die reibungslose Durchführung sichergestellt werden.
Kundenfokus	Von der überwiegenden Anzahl der in der vertiefenden Studie befragten Unternehmen wurde angeführt, dass der Schutzbedarf dann besonders hoch ist, wenn sensitive Inhalte von Kunden verarbeitet werden. Somit sind Prozesse bzw. Projekte, die diese Charakteristika aufweisen, besonders kritisch, da bei einer Verletzung erhebliche Umsatzeinbußen und Reputationsschäden drohen können.
Involvierung externer Partner	Der Schutzbedarf von Prozessen bzw. Projekten nimmt auch dann zu, wenn externe Partner wie Kunden, Lieferanten oder Kooperationspartner in die Aktivitäten involviert sind. Im Rahmen der verschiedenen empirischen Teilstudien wurde auf verschiedenste Risiken, die sich aus einer Offenlegung sensitiver Inhalte oder der bloßen Zusammenarbeit mit externen Partnern ergeben, hingewiesen.
Anteil zu schützender wissensbezogener Ressourcen	Wie in Abschnitt 8.1 dargelegt, können wissensbezogene Ressourcen anhand verschiedener Kriterien, die den unternehmensinternen und –übergreifenden Wert repräsentieren, eingeordnet werden. Werden in den Prozessen bzw. Projekten vergleichsweise viele Ressourcen mit einem hohen Schutzbedarf eingesetzt, so ist auch der Schutzbedarf des Prozesses bzw. Projektes hoch.

Tab. 93 Kriterien zur Beurteilung des Schutzbedarfes (Prozess- und Projektprofile)

Zum anderen sind spezifische Einflussfaktoren, die auf Basis der Literatur und der verschiedenen empirischen Teilstudien identifiziert wurden, von Relevanz und in Tab. 93 zusammengefasst. Neben der

[397] Dies könnte auch auf andere Branchen zutreffen, in denen dem Qualitätsmanagement eine hohe Bedeutung zukommt. So sind beispielsweise Unternehmen anzuführen, die Initiativen zu Six Sigma oder EFQM eingeführt haben oder z.B. nach ISO 9001 oder ISO/TS 16949 zertifiziert sind.

Übersetzung dieser Anforderungen durch die Prozess- und Projektmanager sollten auf der operativen Ebene auch die Kernprozesse des Wissensrisikomanagements verankert sein. So haben die Analysen in Abschnitt 7.5 gezeigt, dass insbesondere die Identifikation und Bewertung der Risiken auf die operative Ebene Vorteile aufweist[398], da die Problemnähe vergleichsweise höher ist und somit eine verbesserte Einschätzung vorgenommen werden kann. Auch für die Steuerung und die Überwachung der Effizienz der Identifikationsverfahren, Bewertungsmethoden und Steuerungsmaßnahmen sollten sich aus analogen Gründen die jeweiligen Prozess- und Projektmanager verantwortlich zeichnen.

Geschäftsprozesse / zusätzliche Funktionen	Zusammenarbeit mit Partnern	Initiierung einer Kooperation	Zusammenarbeit in Projekten	Mitarbeiter freisetzen
Wissenstransfer kontrollieren	●			
Geheimhaltung vereinbaren	●			
Wissen dokumentieren	●		●	
dokumentiertes Wissen validieren	●		●	
Zugriffsrechte anpassen				●
Eignung des Partners überprüfen		●		
gewerbliche Schutzrechte implementieren	●			
Nachfolge planen				●
Redundanz schaffen	●		●	

Abb. 46 wissensrisikoorientierte Erweiterung von Geschäftprozessen

Im Hinblick auf die Implementierung der verschiedenen Steuerungsmaßnahmen zur Reduktion von Wissensrisiken in den operativen Geschäftsprozessen kann eine Verankerung durch eine Integration zusätzlicher Funktionen erfolgen. In Abb. 46 sind exemplarisch die vier Prozesse Zusammenarbeit mit Partnern, Initiierung einer Kooperation, Zusammenarbeit in Projekten und Mitarbeiter freisetzen abgetragen. Zusätzlich sind verschiedene Funktionen, die Aspekte der in den Abschnitten 5.10.2-5.10.4 erörterten Steuerungsmaßnahmen enthalten, abgetragen. Der Prozess Zusammenarbeit mit Partnern kann gemeinsame Produktentwicklung mit Kunden oder Lieferanten oder allgemein den unternehmensübergreifenden Austausch sensitiver Inhalte betreffen. Aufgrund der Sensitivität kann eine Kontrolle des Wissenstransfers im Sinne der Steuerungsmaßnahmen SO6 bzw. SO14 erforderlich sein. Ebenso sind im Rahmen der Produktentwicklung Geheimhaltungsvereinbarungen im Sinne von SR1 relevant, weshalb deren Implementierung über eine entsprechende Funktion in die Prozesse integriert werden könnte. Um weiteren rechtlichen Schutz zu erhalten, könnte der Prozess auch um die Ergreifung gewerblicher Schutz-

[398] Siehe hierzu auch Abschnitt 3.5.2.

rechte (SR6) erweitert werden. Neben der Kontrolle der Transferprozesse und dem Ergreifen von Schutzmaßnahmen kann auch die Verbesserung des Wissenstransfers oder die Sicherung der Wissensqualität ein Gegenstand dieses Prozesses sein. So kann gezielt Wissen, das aufgrund der Klassifikation transferierbar ist, im Sinne der Redundanzschaffung (SO13) verteilt werden oder dokumentiertes Wissen vor der Nutzung validiert werden (SO26). Um gemeinsame Ergebnisse der Zusammenarbeit gegen Wissensverluste zu sichern, kann in den Prozess auch eine Funktion zur Dokumentation von Wissen (SO17) integriert werden. Im Rahmen der Initiierung einer Kooperation, die beispielsweise bauliche und finanzielle Aspekte einschließt, ist aus Sicht des Managements von Wissensrisiken die Auswahl des Kooperationspartners (SO21) von Relevanz. So kann im Konkreten das Verhalten des potentiellen Kooperationspartners in vorangegangenen Kooperationen oder die Komplementarität der Wissensbasen überprüft werden. In die Prozesse der unternehmensinternen Zusammenarbeit in Projekten könnte aus Sicht des Managements von Wissensrisiken zum einen die Dokumentation von Wissen (SO17) zu verschiedenen Meilensteinen oder die Validierung extern bezogenen Wissens (SO26) integriert werden, um Wissensverlusten vorzubeugen bzw. die Qualität des genutzten Wissens sicherzustellen. Zur Verbesserung des unternehmensinternen Wissenstransfers in den Projekten können weiterhin gezielt Maßnahmen zur Redundanzschaffung ergriffen werden. Im Falle einer Freisetzung eines Mitarbeiters können zur Erweiterung dieses Prozesses die Anpassung von Zugriffsrechten im Sinne eines Entzugs (SO11/ ST6) in den Prozess integriert werden. Weiterhin kann bei Bekanntwerden des Austritts die Nachfolgeplanung (SO18) angestoßen werden, um Wissensverluste aus dieser Fluktuation möglichst gering zu halten.

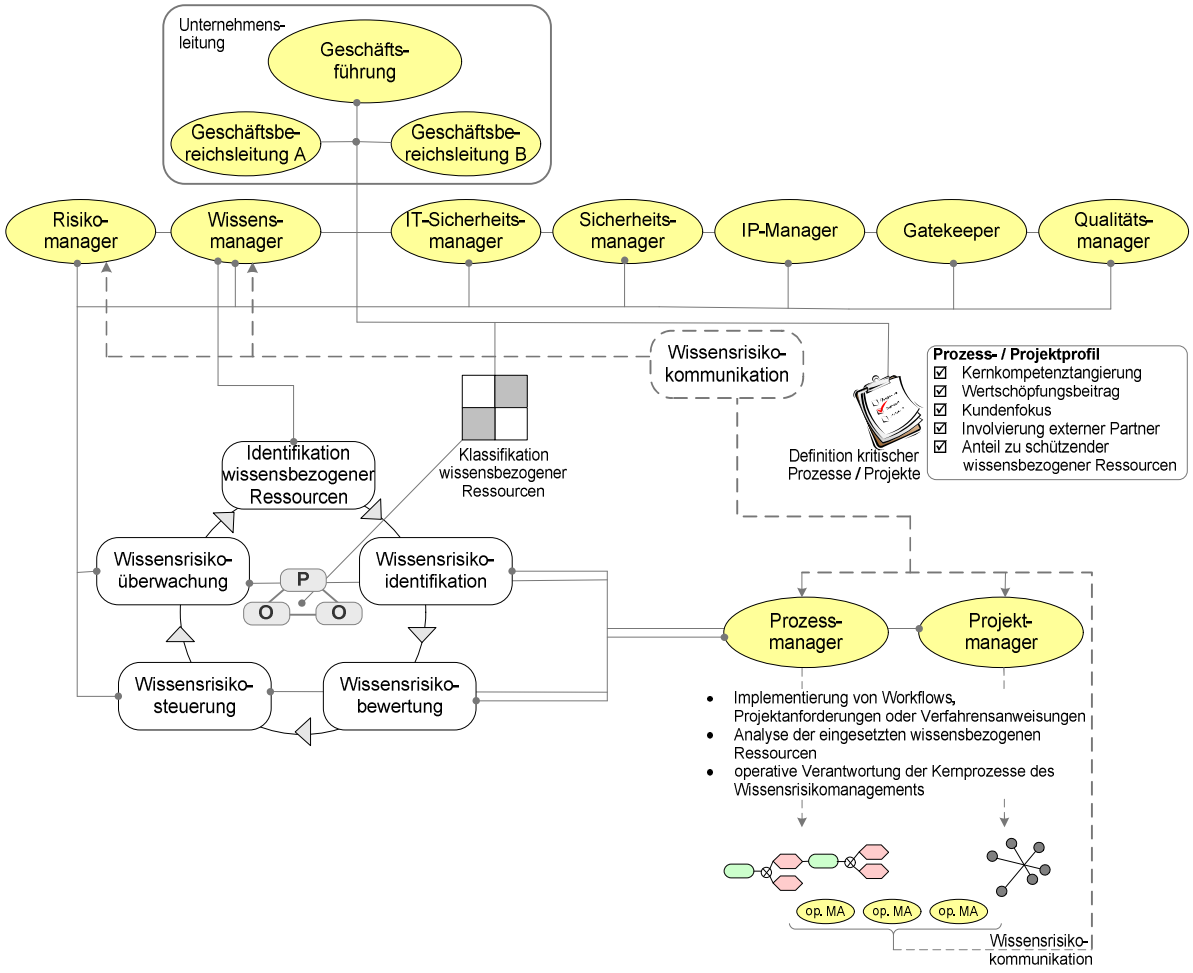


Abb. 47 Implementierungskonzept zum Management von Wissensrisiken

Neben den in Abb. 46 abgetragenen Erweiterungen können eine Vielzahl weiterer operativer Prozesse um weitere Funktionen, die Steuerungsmaßnahmen aus den Abschnitten 5.10.2-5.10.4 umfassen, erweitert werden.

Die Berichterstattung zu Wissensrisiken als Gegenstand der Wissensrisikokommunikation sollte ausgehend von den operativ tätigen Mitarbeitern über die jeweiligen Prozess- und Projektmanager an den Risiko- und Wissensmanager erfolgen, da diesen beiden Rollen aufgrund ihrer fachlichen Ausrichtung das Management der Wissensrisiken besonders gut beurteilen können dürften. Risiko- und Wissensmanager sollten in Abstimmung mit der Unternehmensleitung aus einer regulatorischen und einer WM-fokussierten Perspektive die Tragfähigkeit der Wissensrisiken festlegen.

Nachdem mögliche Ansatzpunkte zur Implementierung des Managements von Wissensrisiken in die Aufbau- und Ablauforganisation von Unternehmen aufgezeigt wurden, wird im nachfolgenden Abschnitt nach einer kurzen Zusammenfassung ein Ausblick auf zukünftigen Forschungsbedarf in diesem Themenkomplex gegeben.

9 Zusammenfassung und Ausblick

Ausgehend von der These, dass sowohl die Risikoorientierung als auch die Bedeutung der Ressource Wissen in den vergangenen Jahren zugenommen haben, wurde das Konzept Wissensrisiko in Anlehnung an den operationellen Risikobegriff erarbeitet. Dabei wurden die Teilkonzepte Wissensverlust, Wissensdiffusion, Wissenstransfer und Wissensqualität erörtert. Auf Basis der Literatur wurden zu diesen Teilkonzepten insgesamt 73 Wissensrisiken in den Ursachenkategorien Personen, Prozesse, Systeme und externe Faktoren identifiziert. Ausgehend von der Literatur zum RM und WM wurde durch eine integrierte Betrachtung der korrespondierenden Ansätze das Konzept Steuerung von Wissensrisiken entwickelt, wobei darüber hinaus zur Identifikation von Steuerungsmaßnahmen Anleihen aus weiteren Forschungsdisziplinen, wie z.B. IT-Sicherheit oder Wirtschaftsspionage, genommen wurden. Insgesamt wurden 45 Steuerungsmaßnahmen identifiziert, die organisatorischer, technischer oder rechtlicher Natur sind und zur Steuerung der 73 Wissensrisiken herangezogen werden können.
Die Zusammenhänge zwischen der Steuerung von Wissensrisiken und den vier abhängigen Konzepten Wissensverlust, Wissensdiffusion, Wissenstransfer und Wissensqualität wurden in einem forschungsleitenden Hypothesenmodell (siehe Abb. 30 auf Seite 252) integriert, das zur Strukturierung der empirischen Studie diente. Auf Basis dieses Modells wurden das Konzept Steuerung von Wissensrisiken und die vier abhängigen Konzepte in insgesamt 36 Variablen operationalisiert und diese in 7 Punkt Likert skalierte Aussagen, die Gegenstand eines Interviewleitfadens sind, überführt. Dabei wurden die beiden Konzepte Wissensverlust und Wissensdiffusion durch negative Variablen und die Konzepte Wissenstransfer und Wissensqualität durch positive Variablen operationalisiert, wobei angenommen wurde, dass eine stärkere Steuerung auf alle vier abhängigen Konzepte einen Risiko vermindernden Einfluss nimmt. Unter Zugrundelegung des Interviewleitfadens wurden auf Basis einer nach Branchen und Größenklassen geschichteten Zufallsstichprobe 129 Unternehmen telefonisch oder schriftlich zu diesen Zusammenhängen befragt. Zur Auswertung wurden deskriptive, induktive und multivariate statistische Verfahren verwendet und dabei v.a. zwischen verschiedenen Teilstichproben signifikante Unterschiede ermittelt. In Bezug auf die verschiedenen Teilstichproben zeigte sich, dass Großunternehmen im Vergleich zu mittelständischen Unternehmen signifikant geringer von Risiken im Kontext des Wissensverlustes und der Wissensdiffusion betroffen sind, während sich in Bezug auf die Teilstichproben produzierender und dienstleistungsorientierter Unternehmen keine signifikanten Unterschiede ergaben. Weitere signifikante Unterschiede bestehen auf Ebene der Konzepte zwischen Unternehmen, die RM- und WM-Initiativen implementiert haben, im Vergleich zu Unternehmen ohne diese Maßnahmen. So weisen Unternehmen mit Maßnahmen in beiden Bereichen eine signifikant höhere Wissensqualität auf und ergreifen zugleich umfassender Steuerungsmaßnahmen (siehe Abschnitt 7.2.7). Durch eine Clusteranalyse wurden vier Gruppen an Unternehmen identifiziert und in

einer vertiefenden Studie je zwei Unternehmen je Cluster erneut zu Zusammenhängen zwischen den Variablen bzw. den identifizierten Faktoren befragt. Weiterhin wurden vier Unternehmen, die durch vergleichsweise positive Ausprägungen über die vier abhängigen Konzepte charakterisiert sind, erneut befragt. Als besonders relevant sind in diesem Fall die Erkenntnisse in Bezug auf unternehmensinterne und -externe Einflussfaktoren anzusehen, die herangezogen werden können, um positive oder negative Ausprägungen der verschiedenen Teilkonzepte zu erklären. Weiterhin wurden diese 12 Unternehmen zu Kriterien zur Klassifikation von Wissen, zu effizienten Steuerungsmaßnahmen zur Begrenzung der Diffusionsrisiken, zu Austauschbeziehungen zwischen der Steuerung und der Hemmung erwünschter Prozesse sowie zur Implementierung des Managements von Wissensrisiken in der Aufbau- und Ablauforganisation des Unternehmens befragt, um über die forschungsleitenden Zusammenhänge hinaus weitere qualitative Erkenntnisse zu gewinnen. Neben der vertiefenden unternehmensübergreifenden Studie wurde auch ein Unternehmen vertiefend untersucht, um Erkenntnisse zur Einschätzung von Wissensrisiken über verschiedene Geschäftsbereiche hinweg und zwischen Führungskräften und Mitarbeitern mit operativen Aufgaben zu gewinnen. Zu diesem Zweck wurde der Interviewleitfaden bei 66 Mitarbeitern des Unternehmens eingesetzt und dabei die Abweichungen zur Unternehmenssicht, die den durch das Unternehmen in der breiten Studie beantworteten Interviewleitfaden darstellt, analysiert. Insgesamt zeigte sich in Bezug auf einige Variablen eine vergleichsweise hohe Spannweite zwischen den 66 Mitarbeitern und der Unternehmensleitung einerseits sowie andererseits über die verschiedenen Teilstichproben. Aufgrund dieser Variabilität erscheint ein unternehmensinterner Einsatz des Interviewleitfadens sinnvoll, da so systematisch Wissensrisiken unter Einbezug verschiedener Perspektiven erhoben werden können.

Die empirisch und auf Basis der Literatur gewonnenen Erkenntnisse wurden abschließend in Handlungsempfehlungen überführt. Dabei wurde zum einen ein Portfolio zur Klassifikation wissensbezogener Ressourcen entwickelt, das zur Bestimmung des Schutzbedarfes dieser Ressourcen dient. Weiterhin wurde als Ergebnis ein Handlungskonzept zur Steuerung von Wissensrisiken entwickelt, das Potentiale der Steuerungsmaßnahmen, Analysen zur Steuerbarkeit der Wissensrisiken, Austauschbeziehungen mit erwünschten Prozessen sowie unternehmensinterne und -externe Einflussfaktoren integriert. Darüber hinaus wurde ein Konzept zur Implementierung des Managements von Wissensrisiken in der Aufbau- und Ablauforganisation entwickelt.

Hinsichtlich der Ergebnisse der einzelnen Kapitel bestehen zum Teil Bedarfe für eine empirische Validierung der Erkenntnisse oder Anknüpfungspunkte für weiterführende Forschung. Diese Aspekte sowie mögliche zukünftige Entwicklungen des Themenkomplexes werden nachfolgend erörtert, um einen Ausblick zu geben.

- **Relevanz des Themengebietes**: Die Durchführung der empirischen Studie hat gezeigt, dass die eingangs vermutete Relevanz des Themengebietes für Unternehmen gegeben ist, was sich insbe-

sondere in positiven Rückmeldungen und Interesse der Ansprechpartner in den Telefoninterviews gezeigt hat. Weiterhin steigt auch das Interesse in der Forschung. So ist im WM zunehmend auch die Betrachtung von Risiken Gegenstand der Forschung, was durch die Etablierung eigener Konferenzen[399] und entsprechender Call for Papers[400] deutlich wird. Ein weiter voranschreitender Wandel zur Wissensgesellschaft und eine immer stärkere Regulation dürften zukünftig ebenso zu wachsendem Interesse beitragen.

- **Forschungsbedarf bzgl. der Teilkonzepte**: Das Konzept Wissensrisiko umfasst nach dem dieser Arbeit zugrunde liegenden Verständnis die vier Teilkonzepte Wissensverlust, Wissensdiffusion, Wissenstransfer und Wissensqualität. Diese sind in unterschiedlichem Umfang beforscht, wobei in Bezug auf die beiden letztgenannten Teilkonzepte umfassende Forschungsergebnisse vorliegen und Wissensverlust und -diffusion vergleichsweise geringer betrachtet wurden. Bezugnehmend auf den wissensbasierten Ansatz und die These, dass die Wertschöpfung und die Generierung von Wettbewerbsvorteilen entscheidend von den wissensbezogenen Ressourcen, über die das Unternehmen verfügt, beeinflusst wird, dürfte zukünftig insbesondere in Bezug auf die beiden Konzepte Wissensverlust und -diffusion weiterer Forschungsbedarf bestehen. Dabei dürfte insbesondere eine vertiefte Analyse von Diffusionsrisiken relevant sein, da sie mit einem Verlust an Exklusivität und somit mit einem potentiellen Wertverlust einhergehen.
- **Limitationen bei der Bewertung**: Wissensrisiken sind in Bezug auf die Risikobewertung durch Limitation gekennzeichnet, die ebenfalls zukünftig Forschungspotential aufweisen dürften. So ist einerseits die Wertbestimmung immaterieller Ressourcen im Allgemeinen und wissensbezogener Ressourcen im Speziellen durch Bewertungsprobleme, die z.B. mit deren Dynamik oder fehlenden Handelbarkeit einhergehen (siehe Abschnitt 2.3), gekennzeichnet. Andererseits sind Wissensrisiken durch eine analoge Problematik wie operationelle Risiken charakterisiert. So liegen im Falle operationeller Risiken im Gegensatz zu traditionellen Risiken keine langjährig aufgebauten Vergangenheitsdaten vor, wodurch die Ermittlung der Eintrittswahrscheinlichkeiten und Schadensausmaße erschwert wird. Bei Wissensrisiken fehlen derartige Vergangenheitsdaten ebenfalls. Zwar können für einige wenige Wissensrisiken, wie z.B. die Mitarbeiterfluktuation oder Personalausfall, Vergangenheitsdaten herangezogen werden, jedoch ist dies für die Mehrheit der in den Abschnitten 5.3-5.6 dargestellten Wissensrisiken zum jetzigen Zeitpunkt nicht möglich, weshalb auch in diesem Bereich zukünftig Forschungsbedarf besteht.
- **Kataloge für Wissensrisiken und Steuerungsmaßnahmen**: In Kapiel 5 wurden 73 Wissensrisiken und 45 Steuerungsmaßnahmen auf Basis der Literatur ermittelt. Zudem wurden exemplarisch

[399] In 2006 wurde der zweite „Workshop on Secure Knowledge Management“ abgehalten. Siehe hierzu auch: http://www.cs.stonybrook.edu/skm2006.

[400] Im Oktober 2007 erschien im Journal „Information Systems Frontiers“ die „Special issue on secure knowledge management“.

ebenfalls auf Basis der Literatur Interaktionen identifiziert und weiterhin eine auf plausiblen Überlegungen basierende Vernetzung der Steuerungsmaßnahmen und Wissensrisiken vorgenommen. Eine systematische Auseinandersetzung mit Wissensrisiken und deren effizienten Steuerung in Unternehmen dürfte zur Ermittlung der Relevanz bestehender sowie zur Identifikation weiterer Risiken und Maßnahmen beitragen. Eine erste Erweiterung dieser Kataloge erfolgte im Rahmen der vertiefenden Studien, in denen zusätzliche Steuerungsmaßnahmen und Varianten zu bestehenden Maßnahmen identifiziert wurden. Ebenso dürfte eine empirische Validierung auch zur Identifikation von Interaktionen, die kumulierende oder kompensierende Wirkungen haben können, sowie zur Gewinnung von Erkenntnissen zur Vernetzung von Steuerungsmaßnahmen und Wissensrisiken beitragen. Derartige Erkenntnisse könnten in nachfolgender Forschung durch den Einsatz eines Werkzeugs gewonnen werden, das am Know-Center[401] in Graz im Kontext einer Diplomarbeit (Moser 2005) entwickelt wurde. Das entwickelte Werkzeug, das eine Vernetzung von Wissensrisiken und Steuerungsmaßnahmen vorsieht und die Identifikation und Bewertung von Wissensrisiken unterstützt, könnte unter Einbezug der in dieser Arbeit identifizierten Kataloge in der Praxis eingesetzt werden, um insbesondere Erkenntnisse zur Relevanz von Wissensrisiken und zur Eignung der Steuerungsmaßnahmen zu gewinnen.

- **Konzentration auf Teilstichproben**: Um eine höhere Repräsentativität der Ergebnisse zu erzielen, wurde die empirische Studie breit ausgerichtet und demzufolge alle Größenklassen und Branchen eingeschlossen. Der durch diese Schichtung erzielte Gewinn an Repräsentativität geht zugleich mit einer vergleichsweise ausgeprägten Heterogenität der betrachteten Unternehmen einher. Aus diesem Grund könnten sich nachfolgende Untersuchungen unter Zugrundelegung der in dieser Studie gewonnenen repräsentativen Erkenntnisse auf einzelne Größenklassen oder Branchen konzentrieren. In Bezug auf die Größenklassen hat die Auswertung der empirischen Studie gezeigt (siehe Abschnitt 7.2.7), dass Großunternehmen vergleichsweise erfolgreicher mit Wissensrisiken umgehen, da sie in Bezug auf die vier abhängigen Konzepte im Vergleich zu den Unternehmen anderer Größenklassen positivere Ausprägungen aufweisen. Bedingt dadurch, dass die Stichprobe nur 22 Großunternehmen einschließt könnten durch nachfolgende Forschung in dieser Teilstichprobe weitere werthaltige Erkenntnisse zum effizienten Umgang mit Wissensrisiken gewonnen werden. Bezüglich Branche bestehen aggregiert betrachtet vergleichsweise geringe Unterschiede (siehe Abschnitt 7.2.7). Bezogen auf die Rückmeldungen in den Telefoninterviews scheint auf der Ebene der Wirtschaftsabschnitte die Relevanz der Thematik im verarbeitenden Gewerbe (WZ-D) vergleichsweise hoch zu sein, während bei dienstleistungsorientierten Unternehmen die Thematik insbesondere bei Unternehmen der Wirtschaftsabschnitte WZ-K und WZ-N auf positive Resonanz gestoßen ist. Weiterhin hat die empirische Studie gezeigt (siehe Abschnitt 7.2.7), dass

[401] http://www.know-center.tugraz.at/

Unternehmen, die sowohl RM- als auch WM-Initiativen implementiert haben, vergleichsweise erfolgreicher mit Wissensrisiken umgehen, was mitunter darauf zurückgeführt werden kann, dass diese Unternehmen vergleichsweise stärker für die Thematik sensibilisiert sind. Aus diesem Grund bietet es sich an, bei weiterführenden Analysen diese Grundgesamtheit heranzuziehen.

- **Konzentration auf Teilkonzepte**: Neben dem breiten Einbezug an Unternehmen wurde in der Studie auch ein breiter Einbezug der verschiedenen Konzepte verfolgt, wobei bedingt durch zeitliche Limitationen der Interviewdurchführung eine Konzentration auf 36 Variablen bzw. 13 Steuerungsmaßnahmen und 23 Wissensrisiken erfolgte. Somit konnte nur ein Teil der in Kapitel 5 dargestellten Wissensrisiken und Steuerungsmaßnahmen in die empirische Studie einbezogen werden. Aus diesem Grund könnte bei einer weitergehenden Studie eine Konzentration auf spezifische Teilkonzepte erfolgen. Bedingt durch die in der Literatur und der vertiefenden Studie identifizierten Austauschbeziehungen zwischen den Konzepten Wissensdiffusion und Wissenstransfer scheint in diesem Bereich hohes Potential für weitergehende Forschung zu bestehen[402]. Weiterhin hat sich in Bezug auf die Steuerbarkeit der Wissensrisiken durch die in der Studie verwendeten Steuerungsmaßnahmen (siehe Abschnitte 7.2.3 und 8.2.2) gezeigt, dass insbesondere Diffusionsrisiken vergleichsweise schlecht steuerbar sind. Auf der anderen Seite weist diese Risikokategorie ein relativ hohes Risikopotential auf, da diese Risiken mit einem Verlust der Exklusivität der Ressourcen und somit potentiell mit einem Wertverlust einhergehen. Bedingt durch diese Defizite in der Steuerung besteht auch an dieser Stelle zukünftig Forschungsbedarf.
- **vertiefte Analyse der Einflussfaktoren**: Die aus der vertiefenden unternehmensübergreifenden Studie gewonnenen Erkenntnisse zu potentiellen unternehmensinternen und -externen Einflussfaktoren in Abschnitt 8.2.4 liefert einen ersten Anhaltspunkt wie positive oder negative Ausprägungen über die vier abhängigen Konzepte zustande kommen können. Dennoch verhindert die geringe Stichprobe von 12 Unternehmen und die Heterogenität der Unternehmen im Hinblick auf Größe, Branchenzugehörigkeit, Wettbewerbsumfeld etc. die Verallgemeinerbarkeit dieser Einflussfaktoren. Aus diesem Grund besteht zukünftig Forschungsbedarf in Bezug auf fokussierte Untersuchungen, bei denen eine Analyse bestimmter Unternehmensgrößen, Branchen oder Unternehmen, die in RM- oder WM-Initiativen implementiert haben, vorgenommen wird.
- **vertiefte Analyse von Austauschbeziehungen**: In Bezug auf den Einfluss einiger Steuerungsmaßnahmen, wie z.B. Wissenstransferrichtlinien, Begrenzung der Interaktion oder Geheimhaltungsvereinbarungen, bestätigten sich die bei der Konzeption der Studie vermuteten negativen Einflüsse bei der quantitativen Auswertung der breiten Studie nicht (siehe Abschnitt 7.3). Die Interviews in der vertiefenden unternehmensübergreifenden Studie zeigten jedoch, dass derartige Austauschbeziehungen von Relevanz sind. Aus diesem Grund könnten im Rahmen aufbauender

[402] Für erste Ansätze für eine detaillierte Untersuchung der Teilkonzepte siehe (Bayer, Maier 2006)

Forschung eine systematische Analyse von Austauschbeziehungen vorgenommen werden, wobei sich eine qualitative fallbasierte Erhebung eignen könnte.

- **Validierung des Portfolios zur Klassifikation**: Der Wissensrisikomanagementprozess kann durch Methoden des traditionellen RM unterstützt werden. In Bezug auf die vorgelagerte Phase Identifikation wissensbezogener Ressourcen, die zugleich die Schnittstelle zum WM darstellt, ist die Klassifikation wissensbezogener Ressourcen bedeutend, um eine Konzentration auf werthaltige Ressourcen vorzunehmen und somit Steuerungsmaßnahmen gezielt zu allokieren. Zu diesem Zweck wurde auf Basis der vertiefenden unternehmensübergreifenden Studie und der Literatur ein erstes Portfolio und entsprechende Kriterien zur Klassifikation der Ressourcen entwickelt. Aufgrund der vergleichsweise geringen Stichprobe von 12 befragten Unternehmen stellt dieser Ansatz zur Klassifikation nur einen ersten Anhaltspunkt dar, der in weiterführender Forschung zu validieren ist.
- **Validierung der Vorschläge zur Implementierung**: Im Hinblick auf die Implementierung des Ansatzes in Unternehmen wurden auf Basis der vertiefenden unternehmensübergreifenden Studie und der Literatur Vorschläge für die Aufbau- und Ablauforganisation entwickelt. Hinsichtlich Aufbauorganisation könnten verteilte Rollen in Unternehmen geschaffen werden, die für spezifische Teilaspekte des Managements von Wissensrisiken verantwortlich sind. Als bedeutend hat sich in den Interviews auch die Verankerung in der Unternehmensleitung herausgestellt. So könnten seitens der Unternehmensleitung strategische Vorgaben gemacht werden, die durch die entsprechenden Rollen sowie Bereichs- und Abteilungsleiter auf den operativen Ebenen kommuniziert werden. Bezüglich Ablauforganisation ist eine Integration des Managements von Wissensrisiken in die operativen Prozesse seitens der Interviewpartner vorstellbar. So könnten Prozessbeschreibungen, Arbeits- oder Verfahrensanweisungen sowie das Projektmanagementhandbuch um Aspekte des Wissensrisikomanagements entsprechend erweitert werden. Analog zur Klassifikation wissensbezogener Ressourcen basieren die gewonnenen Erkenntnisse nur auf einer vergleichsweise geringen Stichprobe (n=12). Aus diesem Grund sind die Vorschläge zur Implementierung als erste Ansatzpunkte zu verstehen, die ebenfalls einer weiterführenden Validierung bedürfen.

Literaturverzeichnis

Abell, A., Oxbow, N. (2002): Competing with Knowledge. The information professional in the knowledge management age. 2.Auflage, London, Library.

ADM (2005): Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.: Richtlinie zum Umgang mit Adressen in der Markt- und Sozialforschung.

Akgün, A. E., Byrne, J. C., Lynn, G. S., Keskin, H. (2007): "Organizational unlearning as changes in beliefs and routines in organizations." in: Journal of Organizational Change Management 20 (6), S.794 - 812.

Al-Laham, A. (2003): Organisationales Wissensmanagement. Stuttgart, Vahlen.

Alberts, C., Dorofee, A. (2003): Managing information security risks: the OCTAVE approach. Boston, Addison-Wesley.

Almeida, P., Song, J., Grant, R. M. (2002): "Are Firms Superior to Alliances and Markets? An Empirical Test of Cross-Border Knowledge Building." in: Organization Science 13 (2), S.147-161.

Alstete, J. (2003): "Trends in Corporate Knowledge Asset Protection." in: Journal of Knowledge Management Practice 4.

Altenburger, O. A. (2003): Risikomanagement für Gründer. in: Dowling, M.,Drumm, H. J. Gründungsmanagement. Vom erfolgreichen Unternehmensstart zum dauerhaften Wachstum. 2.Auflage, Berlin, Springer, S.147-161.

Alter, S. (2006): Goals and Tactics on the Dark Side of Knowledge Management. in: Proceedings of the 39th Hawaii International Conference on System Sciences - 2006, S.1-10.

Alvesson, M. (2001): "Knowledge work: Ambiguity, image and identity." in: Human Relations 54 (7), S.863-886.

Alvesson, M. (2004): Knowledge work and knowledge-intensive firms. Oxford, Oxford Univ. Press.

Alwert, K. (2005): Wissensbilanzen - Im Spannungsfeld zwischen Forschung und Praxis. in: Mertins, K., Alwert, K.,Heisig, P. Wissensbilanzen. Intellektuelles Kapital erfolgreich nutzen und entwickeln. Heidelberg, Springer, S.19-39.

Alwert, K., Heisig, P., Mertins, K. (2005): Wissensbilanzen. Intellektuelles Kapital erfolgreich nutzen und entwickeln. in: Mertins, K., Alwert, K.,Heisig, P. Wissensbilanzen. Intellektuelles Kapital erfolgreich nutzen und entwickeln. Heidelberg, Springer, S.1-17.

Amelingmeyer, J. (2002): Wissensmanagement: Analyse und Gestaltung der Wissensbasis von Unternehmen. 2.Auflage, Wiesbaden, DUV.

Amelingmeyer, J. (2004): Wissensmanagement: Analyse und Gestaltung der Wissensbasis von Unternehmen. 3.Auflage, Wiesbaden, DUV.

Andersson, D., Norrman, A. (2004): Outsourcing Advanced logistics: A Shipper's and Provider's Persective on Risks. in: Brindley, C. Supply chain risk. Aldershot, Ashgate, S.160-174.

Andrews, K. R. (1971): The concept of corporate strategy. Homewood, Dow Jones-Irwin.

Andriessen, D. (2004): "IC valuation and measurement: classifying the state of the art." in: Journal of Intellectual Capital 5 (2), S.230-242.

Ansoff, I. (1965): Corporate strategy: an analytic approach to business policy for growth and expansion. New York, McGraw-Hill.

Antoni, C. H., Sommerlatte, T. (2001): Spezialreport Wissensmanagement. Wie deutsche Firmen ihr Wissen profitabel machen. Düsseldorf, Symposion.

Anwander, A. (2002): Strategien erfolgreich verwirklichen. Wie aus Strategien echte Wettbewerbsvorteile werden. Berlin, Springer.

Appleyard, M. M., Kalsow, G. M. (1999): "Knowledge diffusion in the semiconductor industry." in: Journal of Knowledge Management 3 (4), S.288-295.

APQC (1996): International Benchmarking Clearinghouse: Knowledge Management Consortium Benchmarking Study, Best Practice Report. Houston, American Productivity & Quality Center.

Arbeitskreis (2000): "Arbeitskreis externe und Interne Überwachung der Unternehmung der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V. Auswirkungen des KonTraG auf die Unternehmensüberwachung - KonTraG und Vorstand - KonTraG und Interne Revision - KonTraG und Aufsichtsrat - KonTraG und Wirtschaftsprüfer." in: Der Betrieb 11 (37), S.1-11.

Arbeitskreis (2001): "Arbeitskreis immaterielle Werte im Rechnungswesen der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V.: Kategorisierung und bilanzielle Erfassung immaterieller Werte." in: Der Betrieb 19, S.989-995.

Arbeitskreis (2002): "Arbeitskreis externe Unternehmensrechnung der Schmalenbachgesellschaft - Grundsätze für das Value Reporting." in: Der Betrieb 55 (45), S.2337-2340.

Arbeitskreis (2003): "Arbeitskreis immaterielle Werte im Rechnungswesen der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V.: Freiwillige externe Berichterstattung über immaterielle Werte." in: Der Betrieb 23, S.1233-1237.

ARC (2005): Austrian Research Centers, Wissensbilanz 2005, Seibersdorf.

Archbold, C. A. (2005): "Managing the bottom line: risk management in policing." in: Policing: An International Journal of Police Strategies & Management 28 (1), S.30-48.

Argote, L., Ingram, P. (2000): "Knowledge Transfer: a Basis for Competitive Advantage in Firms." in: Organizational Behavior and Human Decision Process 82 (1), S.150-169.

Argyris, C., Schön, D. (1978): Organizational Learning - A Theory of Action Perspective. Reading, Addison-Wesley.

Arrow, K. J. (1962): "The Economic Implications of Learning by Doing." in: The Review of Economic Studies 29 (3), S.155-173.

Asllani, A., Luthans, F. (2003): "What knowledge managers really do: an empirical and comparative analysis." in: Journal of Knowledge Management 7 (3), S.53 - 66.

Atherton, M. (2007): Managing Information Risk - An assessment of progress, Executive Insight Report, URL: http://www.freeformdynamics.com, letzter Zugriff: 14.03.2008.

Aubert, B. A., Patry, M., Rivard, S. (2002): Managing IT Outsourcing Risk: Lessons Learned. in: Hirschheim, R. Information systems outsourcing: enduring themes, emergent patterns and future directions. Berlin, Springer, S.155-176.

Aulinger, A. (1996): (Ko-)Operation Ökologie – Kooperationen im Rahmen ökologischer Unternehmenspolitik. Marburg, Metropolis.

Awazu, Y. (2004a): "Informal network players, knowledge integration, and competitive advantage." in: Journal of Knowledge Management 8 (3), S.62-70.

Awazu, Y. (2004b): "Informal Roles and Intelligence Activities: Some Management Propositions." in: Journal of Competitive Intelligence and Management 2 (1), S.16-24.

Awazu, Y., Desouza, K. C. (2004): "Chief Privacy Officers." in: Edpacs (3), S.23-24.

Ayliffe, R. (2005): Risks in the supply chain. in: Reuvid, J. Managing Business Risk. A practical guide to protecting your business. London, Kogan Page, S.47-51.

Bach, N., Homp, C. (1997): Wissensmanagement als Querschnittsaufgabe des Kernkompetenzmanagements, Arbeitspapier Nr. 3/1997 des Lehrstuhls für Betriebswirtschaftslehre II, Justus-Liebig-Universität Gießen.

Bach, V., Österle, H., Vogler, P. (2000): Business Knowledge Management in der Praxis. Prozessorientierte Lösungen zwischen Knowledge Portal und Kompetenzmanagement. Berlin, Springer.

Bach, V., Vogler, P., Österle, H. (1999): Business Knowledge Management. Praxiserfahrungen mit Intranet-basierten Lösungen. Berlin, Springer.

Backhaus, K., Erichson, B., Plinke, W., Weiber, R. (2006): Multivariate Analysemethoden: eine anwendungsorientierte Einführung. Berlin, Springer.

Badaracco, J. L. (1991): Strategische Allianzen: wie Unternehmen durch Know-how-Austausch Wettbewerbsvorteile erzielen. Wien, Ueberreuter.

Baer, R., Zängerle, P. (2000): "Wie misst man IT-Sicherheit?" in: HMD - Praxis der Wirtschaftsinformatik 216 (12), S.67-77.

Bain, J. S. (1968): Industrial organization. New York, Wiley.

Bamberger, I., Wrona, T. (1996): "Der Ressourcenansatz im Rahmen des Strategischen Managements." in: WiSt - Wirtschaftswissenschaftliches Studium 25 (8), S.386-391.

Barney, J. B. (1991): "Firm Resources and Sustained Competitive Advantage." in: Journal of Management 17 (1), S.99-120.

Barth, S. (2001): "Open Yet Guarded: Protecting the Knowledge Enterprise." in: Knowledge Management Magazine, März 2001.

Barthel, E., Gieri, R., Kühn, I.-W. (2004): Humankapital in Unternehmen - Ansätze zur Bewertung. in: Hasebrook, J., Zawacki-Richter, O.,Erpenbeck, J. Kompetenzkapital: Verbindungen zwischen Kompetenzbilanzen und Humankapital. Frankfurt a. M., Bankakad, S.17-50.

Basel (2003): Baseler Ausschuss für Bankenaufsicht. Management operationeller Risiken - Praxisempfehlungen für Banken und Bankaufsicht, Basel.

Basel (2004): Baseler Ausschuss für Bankenaufsicht, Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen - überarbeitete Rahmenvereinbarung-, Juni 2004, Basel.

Basel (2005): Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards, Basel.

Baughn, C., Denekamp, J., Stevens, J., Osborn, R. (1997): "Protecting intellectual capital in international alliances." in: Journal of World Business 32 (2), S.103–117.

Bayer, F., Enparantza, R., Maier, R., Obermair, F., B., S. (2005): Know-CoM: Decentralized Knowledge Management Systems for Cooperating Die and Mold Making SMEs. in: Jennex, E. M. Case Studies in Knowledge Management. Hershey, S.186-209.

Bayer, F., Maier, R. (2006): Knowledge Risks in Inter-Organizational Knowledge Transfer in: Tochtermann, K, Maurer, H.: Proceedings of I-Know ’06, 6th International Conference on Knowledge Management, Graz, 6.-8. September 2006, S. 76-84.

Bea, F. X., Haas, J. (2005): Strategisches Management. Stuttgart, Lucius & Lucius.

Becker, M. C., Knudsen, M. P. (2003): Barriers and managerial challenges to knowledge transfer processes. in: DRUID Summer Conference 2003, Kopenhagen.

Beier, H. (2004): "Vom Wort zum Wissen. Semantische Netze als Mittel gegen die Informationsflut." in: Information Wissenschaft und Praxis 55 (3), S.133-138.

Beier, H. (2005): "Welt im Wandel: Wissen tut Not." in: BIT 6 (1), S.45-54.

Belsis, P., Kokolakis, S., Kiountouzis, E. (2005): "Information systems security from a knowledge management perspective." in: Information Management & Computer Security 13 (3), S.189-202.

Bender, R., Lange, S. (2001): "Adjusting for multiple testing-when and how?" in: Journal of Clinical Epidemiology 54, S.343-349.

Bhatt, G. D. (2001): "Knowledge management in organizations: examining the interaction between technologies, techniques, and people." in: Journal of Knowledge Management 5 (1), S.68-75.

Bieta, V. (2002): Risikomanagement und Spieltheorie: wie Global Player mit Risiken umgehen müssen. Bonn, Galileo Press.

Bitkom (2003): Bitkom: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien, Sicherheit für Systeme und Netze in Unternehmen. Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen. URL: http://www.bitkom.org/files/documents/ACF897.pdf, letzter Zugriff: 14.03.2008.

Bitkom (2005): Kompass der IT Sicherheitsstandards. Ein Leitfaden für mittelständische Unternehmen. URL: http://www.bitkom.org/de/publikationen/1357.aspx, letzter Zugriff: 14.03.2008.

Bitkom (2006): Kompass der IT-Sicherheitsstandards. Leitfaden und Nachschlagewerk. URL: http://www.bitkom.de/de/themen_gremien/36729_31037.aspx, letzter Zugriff: 14.03.2008.

Bitz, H. (2000): Risikomanagement nach KonTraG: Einrichtung von Frühwarnsystemen zur Effizienzsteigerung und zur Vermeidung persönlicher Haftung. Stuttgart, Schäffer-Poeschel.

Blackler, F. (1995): "Knowledge, Knowledge Work and Organizations: An Overview and Interpretation." in: Organization Studies 16 (6), S.1021-1046.

Bleeke, J., Ernst, D. (1993): Collaborating to compete: using strategic alliances and acquisitions in the global marketplace. New York, Wiley.

Blind, K., Cremers, K., Mueller, E. (2007): The Influence of Strategic Patenting on Companies' Patent Portfolios, Discussion Paper No. 07-013, Centre for Economic European Research.

Blommestein, H. J. (2005): Overview of RISK Management Practices in OECD Countries. in. OECD, Organisation for Economic Co-operation and Development. Advances in risk management of government debt. Paris, OECD Publ., S.27-37.

BMWI (2006): Bundesministerium für Wirtschaft und Technologie, Wissensbilanz – Made in Germany, Leitfaden 1.0 zur Erstellung einer Wissensbilanz, Berlin.

Bonora, E. A., Revang, Ø. (1993): A Framework for Analysing the Storage and Protection of Knowledge in Organizations - Strategic Implications and Structural Arrangements. in: Lorange, P., Chakravarthy, B., Roos, J.,Van de Ven, A. Implementing Strategic Processes. Oxford, Blackwell, S.190-213.

Bönte, W., Wiethaus, L. (2005): Knowledge Transfer in Buyer-Supplier Relationships- When It (Not) Occurs, RWI: Discussion Papers No.34.

Bontis, N. (1996): "There's a price on your head: managing intellectual capital strategically." in: Ivey Business Quarterly 18 (4), S.40-47.

Book, N., Rudolph, D. (2005): "IT-Risk Management -Sarbanes-Oxley & Co. als Motor der IT-Sicherheit?" in: Information Management & Consulting 20 (2), S.55–60.

Bortz, J. (2005): Statistik: für Human- und Sozialwissenschaftler. 6.Auflage, Berlin, Springer.

Bortz, J., Döring, N. (2005): Forschungsmethoden und Evaluation: für Human- und Sozialwissenschaftler. 3.Auflage, Heidelberg, Springer.

Bortz, J., Lienert, G. (2000): Verteilungsfreie Methoden in der Biostatistik. Berlin, Springer.

Bovee, M., Srivastava, R. P., Mak, B. (2003): "A Conceptual Framework and Belief-Function Approach to Assessing Overall Information Quality." in: International Journal of Intelligent Systems 18, S.51-74.

Braun, H. (1984): Risikomanagement: eine spezifische Controllingaufgabe. Darmstadt, Toeche-Mittler.

Broda, B. (2003): "Alternative Ansätze zur Messung des intellektuellen Kapitals." in: Der Schweizer Treuhänder (9), S.729-740.

Brooking, A. (1996): Introduction to Intellectual Capital. Cambridge.

Brown, J. S., Duguid, P. (1998): "Organizing Knowledge." in: California Management Review 40 (3), S.90-111.

Brown, W., Nasuti, F. (2005): "Sarbanes-Oxley and Enterprise Security: IT Governance - What it Takes to Get the Job Done." in: Security Management Practices 14 (5), S.15-28.

Bruns, G., Thuy, M. G., Zeimes, M. (2003): "Die Bilanzierung von immateriellen Vermögenswerten des Anlagevermögens und Goodwill im Konzernabschluss. Gemeinsamkeiten und Unterschiede der deutschen, US-amerikanischen und internationalen Rechnungslegung." in: Controlling (3/4), S.137-142.

Bryman, A., Bell, E. (2003): Business research methods. Oxford, Oxford Univ. Press.

BSI (2006): IT-Grunschutz-Kataloge, URL: http://www.bsi.bund.de/gshb/deutsch/download/, letzter Zugriff: 14.03.2008.

Buhr, R. (2000): "Messung von Betriebsrisiken - ein methodischer Ansatz." in: Die Bank (3), S.202-206.

Bukh, P. N., Mourtisen, J., Christensen, K. S. (2005): Intellectual Capital: Managing and Reporting Knowledge resources. in: Bukh, P. N.,Christensen, K. S. Knowledge management and intellectual capital: establishing a field of practice. Basingstoke, Palgrave Macmillan, S.53-69.

Bullinger, H. J., Wörner, K., Prieto, J. (1997): Wissensmanagement heute. Daten, Fakten, Trends, Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO), Stuttgart.

Burger, A., Buchhart, A. (2002): Risiko-Controlling. München, Oldenbourg.

Burgess, M. S. E., Gray, W. A., Diddian, N. J. (2004): Quality Measures and the Information Consumer, in: Proceedings of the Ninth International Conference on Information Quality (ICIQ 04). Cambridge, S.373-388.

Burghardt, M. (2002): Projektmanagement: Leitfaden für die Planung, Überwachung und Steuerung von Entwicklungsprojekten., Erlangen, Publicis Corp. Publ.

Bussmann, K. F. (1955): Das betriebswirtschaftliche Risiko. Meisenheim am Glan, Hain.

Capgemini (2005): Infrastruktur ohne große Bedeutung für immaterielles Vermögen eines Unternehmens, Berlin.URL: http://www.de.capgemini.com/presse/pressemitteilungen/archiv_2005/CFO_Trends/, letzter Zugriff: 14.03.2008.

Carlucci, D., Schiuma, G. (2006): "Knowledge Asset Value Spiral: Linking Knowledge Assets to Company's Performance." in: Knowledge and Process Management 13 (1), S.35-46.

Carrión, G. C., González, J. L. G., Leal, A. (2004): "Identifying key knowledge area in the professional services industry: A case study." in: Journal of Knowledge Management 8 (6), S.131-150.

CC (2006a): Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1.

CC (2006b): Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1.

CC (2006c): Common Criteria for Information Technology. Security Evaluation Part 1: Introduction and general model, Version 3.1.

Chandler, A. D. (1962): Strategy and structure: chapters in the history of the industrial enterprise. Cambridge, MIT Press.

Chase, R. L. (1997): "The Knowledge-Based Organization: An International Survey." in: Journal of Knowledge Management 1 (1), S.38-49.

Cheung, S. C., Chiu, D. K. W. (2003): A Watermarking Infrastructure for Enterprise Document Management, in Proceedings of the 36th Hawaii International Conference on System Sciences (HICCS ´03).

Child, J. (2001): Learning through Strategic Alliances. in: Dierkes, M. Handbook of Organizational Learning and Knowledge. Oxford, Oxford Univ. Press.

Child, J., Faulkner, D. (1998): Strategies of cooperation: managing alliances, networks, and joint ventures. New York, Oxford Univ. Press.

Chmielewicz, K. (1979): Forschungskonzeptionen der Wirtschaftswissenschaft. 2.Auflage, Stuttgart, Poeschel.

Choi, C. J., Cheng, P., Hilton, B., Russell, E. (2005): "Knowledge governance." in: Journal of Knowledge Management 9 (6), S.67-75.

Churchill, G. A. (1979): "A Paradigm for Developing better Measures of Marketing Constructs." in: Journal of Marketing Research 16 (2), S.64-73.

Civi, E. (2000): "Knowledge management as a competitive asset: a review." in: Marketing Intelligence & Planning 18 (4), S.166-174.

Claflin, B. (2001): "Information Risk Management at 3Com." in: Security Business Quaterly 1 (2), S.1-2.
Clarke, T. (2001): "The knowledge economy." in: Education + Training 45 (4/5), S.189-196.
Coase, R. H. (1937): The nature of the firm. in. Economica. Oxford, Blackwell, S.386-405.
Cohen, W. M., Levinthal, D. A. (1990): "Absorptive Capacity: A New Perspective on Learning and Innovation." in: Administrative Science Quaterly 35 (1), S.128-152.
Coleman, L., Casselman, R. M. (2004): What You Don't Know Can Hurt You: Towards an Integrated Theory of Knowledge and Corporate Risk. Working Paper 2004/10011, Melbourne.
Collins, J., Vile, D. (2007): Enabling the Trusted Workforce. A balanced approach to managing people related risk, Executive Insight Report, URL: http://www.freeformdynamics.com, letzter Zugriff: 14.03.2008.
Connor, K. R., Prahalad, C. K. (1996): "A Resource-based Theory of the Firm: Knowledge versus Opportunism." in: Organization Science 7 (7), S.477 -501.
Contractor, F. (2000): "Valuing corporate Knowledge and Intangible Assets: Some General Principles." in: Knowledge and Process Management 7 (4), S.242-255.
Cougias, D. (2003): The Backup book: disaster recovery from desktop to data center. Lecanto, Schaser-Vartan Books.
Cross, R., Prusak, L. (2002): "The People who make organizations Go or Stop." in: Harvard Business Review 80 (6), S.104-112.
Cruz, M. G. (2002): Modeling, measuring and hedging operational risk. Chichester, Wiley.
CSI/FBI (2005): Computer Crime and Security Survey 2005. Computer Security Institute Publications, URL: http://www.GoCSI.com, letzter Zugriff: 14.03.2008.
Culp, C. L., Mensink, R. (2003): Measuring risk for asset allocation, performance evaluation, and risk control: different problems, same solution. in: Warwick, B. The Handbook of risk. Hoboken, Wiley.
Cummings, J. (2003): Knowledge Sharing: A Review of the Literature. The World Bank, Washington, D.C.http://lnweb18.worldbank.org/oed/oeddoclib.nsf/DocUNIDViewForJavaSearch/D9E389E7414BE9DE85256DC600572CA0/$file/knowledge_eval_literature_review.pdf, letzter Zugriff: 14.03.2008.
Cummings, J. L., Teng, B. S. (2003): "Transferring R&D knowledge - the key factors affecting knowledge transfer success." in: Journal of Engineering and Technology Management 20 (1), S.39-68.
Daft, R. L., Lengel, R. H. (1986): "Organizational information requirements, media richness and structural design." in: Management Science 32 (5), S.554-571.
Das, T. K. (2005): "Deceitful behaviors of alliance partners: potential and prevention." in: Management Decision 43 (5), S.706-719.
Das, T. K., Teng, B.-S. (1999): "Managing risks in strategic alliances." in: Academy of Management Executive 13 (4), S.50-62.
Davenport, D. L., Holsapple, C. W. (2006): Knowledge Organizations. in: Schwartz, D. G. Encyclopedia of knowledge management. Hershey, Idea Group, S.451-458.
Davenport, T. H., Prusak, L. (1998): Working knowledge: how organizations manage what they know. Boston, Harvard Business School Press.
Davies, W. (2000): Partner Risk: Managing the Downside of Strategic Alliances. West Lafayette, Purdue Univ. Press.
De Clercq, J., Rouault, J. (2004): An Introduction to Identity Management. http://devresource.hp.com/drc/resources/idmgt_intro/idmgt_intro.pdf, letzter Zugriff: 14.03.2008.

de Laat, P. B. (1999): Dangerous liasions- Sharing knowledge within research and development alliances. in: Grandori, A. Interfirm Networks. Organization and Industrial Competitiveness. London, Routledge, S.208-233.
De Vries, H. (2006): IT Standards Typology. in: Jakobs, K. Advanced Topics in Information Technology Standards and Standardization Research Volume I. Hershey, Idea Group, S.1 - 26.
Deking, I. (2003): Management des Intellectual Capital. Bildung einer strategiefokussierten Wissensorganisation. Wiesbaden, DUV.
DeLoach, J. W. (2000): Enterprise-wide risk management: strategies for linking risk and opportunity. London, Financial Times Prentice Hall.
Deloitte (2005): 2005 Global Security Survey, URL: http://www.deloitte.com/dtt/research/0,1015,sid=1013&cid=85452,00.html, letzter Zugriff: 14.03.2008.
Delphi (1997): Delphi On Knowledge Management. Research & Perspectives on Today's Knowledge Landscape, Boston.
DeMarco, T., Lister, T. (2003): Bärentango. Mit Risikomanagement Projekte zum Erfolg führen. München, Hanser.
DeNisi, A. S., Hitt, M., A., Jackson, S. E. (2003): The Knowledge-Based Approach to Sustainable Competitive Advantage. in: Jackson, S. E., Hitt, M. A.,DeNisi, A. S. Managing Knowledge for Sustained Competitive Advantage: Designing Strategies for Effective Human Resource Management. San Francisco, John Wiley & Sons, S.3-33.
Desouza, K. C., Awazu, Y. (2004): "Securing knowledge assets." in: J@pan.Inc 58 (8).
Desouza, K. C., Awazu, Y. (2005): "Segment and destroy: the missing capabilities of knowledge management." in: Journal of Business Strategy 26 (4), S.46-52.
Desouza, K. C., Awazu, Y. (2006): "Knowledge management at SMEs: five peculiarities." in: Journal of Knowledge Management 10 (1), S.32-43.
Desouza, K. C., Vanapalli, G. K. (2005): Securing Knowledge in Organizations. in: Desouza, K. C. New frontiers of knowledge management. Basingstoke, Palgrave Macmillan, S.76-98.
Diederichs, M., Form, S., Reichmann, T. (2004): "Standard zum Risikomanagement." in: Controlling 16. (4/5), S.189-198.
Diederichs, M., Kaminski, M. (2003): "DV-gestütztes Chancen- und Risikomanagement. KonTraG-konformes Balanced Chance- & Risk-Reporting mit Hilfe moderner Informationstechnologien." in: Controlling (12), S.699-709.
Diekmann, A. (1999): Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen. 5.Auflage, Reinbek, Rowohlt-Taschenbuch.
Dierickx, I., Cool, K. (1989): "Asset stock accumulation and sustainability of competitive advantage." in: Management Science 35 (12), S.1504 - 1511.
Dierstein, R. (2004): "Sicherheit in der Informationstechnik - der Begriff IT-Sicherheit." in: Informatik Spektrum 27 (4), S.343-353.
Dillerup, R., Göttert, S. (2005): "Wissensbilanz und Quantifizierung immaterieller Vermögensgegenstände." in: VDMA Nachrichten (12), S.59-60.
Dillerup, R., Ramos, J. (2006): "Steuerung und Bilanzierung immaterieller Vermögenswerte." in: Controller Magazin 28 (2), S.116-119.
Disterer, G. (2002): "Management of project knowledge and experiences." in: Journal of Knowledge Mangement 6 (5), S.512-520.
Dixon, N. M. (2000): Common knowledge: how companies thrive by sharing what they know. Boston, Harvard Business School Press.
DLR (2001): "Deutsches Luft- und Raumfahrtzentrum, Wissensbilanz 2001." in.

Doering, H.-U. (2001): Operational risks in financial services. An old challenge in a new environment. Credit Suisse Group. URL: http://www.credit-suisse.com/en/csgn/operational_risk.pdf, letzter Zugriff: 14.03.2008.
Döring-Katerkamp, U., Trojan, J. (2000): Umfrageergebnisse der Studie "Wissensmanagement in der Praxis". URL: http://www.ifem.org/artikel.htm, letzter Zugriff: 14.03.2008.
Döring-Katerkamp, U., Trojan, J. (2001): Etablierung von Wissensmanagement 2001 - Auswertungen zur Umfrage. URL: http://www.ifem.org/artikel.htm, letzter Zugriff: 14.03.2008.
Dreger, W. (1998): Counter intelligence: betriebliche Spionage-Abwehr; so schützen Sie Ihr Firmen-Know-how gegen Ausspähung durch die Konkurrenz. Renningen-Malmsheim, Expert.
Drucker, P. (1959a): Landmarks of tomorrow. New York, Harper & Brothers.
Drucker, P. (1959b): "Long-Range Planning: Challenge to Management Science." in: Management Science 5 (3), S.238-249.
Drucker, P. (1969): The age of discontinuity: guidelines to our changing society. New York, Harper & Row.
Drucker, P. (1992): "The new society of organizations." in: Harvard Business Review 70 (5), S.95-104.
Drumm, H. J. (2000): Personalwirtschaft. 4.Auflage, Berlin, Springer.
DTI (2004): Information security breaches survey 2004, URL: http://www.infosec.co.uk/files/DTI_Survey_Report.pdf, letzter Zugriff: 14.03.2008.
Dyer, J. H., Nobeoka, K. (2000): "Creating and managing a high-performance knowledge-sharing network: The Toyota case." in: Strategic Management Journal 21 (3), S.345-367.
Eckert, C. (2003): IT-Sicherheit: Konzepte, Verfahren, Protokolle. 2.Auflage, München, Oldenbourg.
Eckert, C. (2006): IT-Sicherheit: Konzepte, Verfahren, Protokolle. 4.Auflage, München, Oldenbourg.
Edvinsson, L. (1997): "Developing Intellectual Capital at Skandia." in: Long Range Planning 30 (3), S.366-373.
Edvinsson, L., Brünig, G. (2000): Aktivposten Wissenskapital: unsichtbare Werte bilanzierbar machen. Wiesbaden, Gabler.
Edvinsson, L., Freij, F. (1999): Skandia: three generations of intellectual capital. in: Imparato, N. Capital for our time: the economic, legal, and management challenges of intellectual capital. Stanford, Hoover Inst. Press, S.192-201.
Edvinsson, L., Malone, M. S. (1997): Intellectual Capital: Realizing your Company's True Value by Finding Its Hidden Brainpower. New York, Harper Business.
EFQM (2005): European Foundation for Quality Management (EFQM) Framework for Risk Management, Brüssel.
Einhaus, C. (2002): "Operationelle Risiken - Grundlagen der aktuellen Diskussion." in: Sparkasse (11), S.488-490.
Elsner, S. H. (2002): Brain Drain! - Der Abfluss von Wissenskapital als Herausforderung an das innerbetriebliche Wissensmanagement. Der Fall der Unternehmensberatung Mummert + Partner. Potsdam, Verl. für Berlin-Brandenburg.
Ensthaler, J. (2003): Gewerblicher Rechtsschutz und Urheberrecht. Berlin, Springer.
Eppler, M. J. (2002): Managing Knowledge Content Quality - Lessons from IT-Analysts, Forschungsbericht, Universität St. Gallen.
Eppler, M. J. (2003a): Das Management der Informationsqualität - Ein Ansatz zur Steigerung des Informationswertes in wissensintensiven Prozessen und Produkten. in: Österle, H.,Winter, R. Business Engineering: Auf dem Weg zum Unternehmen des Informationszeitalters. 2.Auflage, Berlin, Springer, S.203-222.
Eppler, M. J. (2003b): Making Knowledge Visible through Knowledge Maps: Concepts, Elements, Cases. in: Holsapple, J. Handbook on Knowledge Management Vol. 1. Berlin, Springer, S.189-205.

Eppler, M. J. (2003c): Managing Information Quality. Increasing the Value of Information in Knowledge-intensive Products and Processes. Berlin, Springer.
Eppler, M. J. (2004): Das Management der Informationsqualität in Neuen Medien. in: Stanoevska-Slabeva, K. The digital economy: Anspruch und Wirklichkeit, Festschrift für Beat F. Schmid. Berlin, Springer, S.323-338.
Eppler, M. J., Muenzenmayer, P. (2003): Measuring Information Quality in the Web Context: A Survey of State-of-the-Art Instruments and an Application Methodology, in: Proceedings of the Seventh International Conference on Information Quality (ICIQ). S.187-198.
Erben, R. F., Romeike, F. (2002): Risk-Management-Informations-Systeme - Potentiale einer umfassenden IT-Unterstützung des Risk Managements. in: Pastors, P. M. Risiken des Unternehmens: vorbeugen und meistern. München, Hampp, S.551-579.
Erdenberger, C. (2001): "Risikomanagement. Möglichkeiten einer pragmatischen Umsetzung in mittelständischen Unternehmen." in: Controller Magazin 26 (1), S.13-17.
Erickson, G. S., Rothberg, H. N. (2005): "Expanding intelligence Capabilities: Downstream Knowledge Targets." in: Journal of Competitive intelligence and Management 3 (2), S.8-15.
Ernst&Young (2004): Global Information Security Survey 2004, URL: http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf, letzter Zugriff: 14.03.2008.
Escribá-Esteve, A., Urra-Urbieta, J. A. (2002): "An analysis of co-operative agreements from a knowledge-based perspective: an integrative conceptual framework." in: Journal of Knowledge Management 6 (4), S.330-346.
Esser, M., Hackenberger, J. (2004): "Bilanzierung immaterieller Vermögenswerte des Anlagevermögens nach IFRS und US-GAAP." in: KoR (10), S.402-414.
EU (2003): Amtsblatt der Europäischen Kommission. Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Brüssel.
EU (2006): Europäische Union, Reporting intellectual capital to augment research, development and innovation in SMEs. Augment Research, Development and Innovation in SMEs. Report to the Commission of the High Level Expert Group on RICARDIS. Brüssel.
Eucken, W. (1965): Die Grundlagen der Nationalökonomie. 8.Auflage, Berlin, Springer.
Faisst, U., Huther, A., Schneider, K. (2002): "Management von operationellen Risiken - Status, Systemanforderungen und Perspektiven (Teil 2)." in: Kredit & Rating Praxis 28 (4), S.22-24.
Faisst, U., Kovacs, M. (2002): Quantifizierung operationeller Risiken - ein Methodenvergleich, Diskussionspapier WI-123, Universität Augsburg,
Faisst, U., Kovacs, M. (2003): "Quantifizierung operationeller Risiken - ein Methodenvergleich." in: Die Bank 43 (5), S.342-349.
Farny, D. (1979): Grundfragen des risk management. in: Risk management - Strategien zur Risikobeherrschung, Bericht von der 5. Kölner BFuP-Tagung am 5. und 6. Oktober 1978 in Leverkusen, S.11-37.
FASB (2001): Special Report: Business and Financial Reporting, Challenges from the New Economy. Financial Accounting Series, Norwalk, Connecticut.
Fauchart, E. (2003): On Knowledge Sharing Patterns among Rival Firms: The Case of Knowledge on Safety. in: DRUID Summer Conference 2003, Kopenhagen, S.1-20.
Feinstein, J. S., Stein, J. (1988): "Employee opportunism and redundancy in firms." in: Journal of Economic Behavior & Organization 10 (4), S.401-414.
Fitz-Enz, J. (2003): Renditefaktor Personal: so messen und erhöhen Sie den ROI ihrer Mitarbeiter. Frankfurt a. M., Campus.
Fitzgerald, M. (2004): At Risks Offshore, in: CIO Online. URL: http://www.cio.com.au/index.php/id;1415953507;fp;fpid;pf;1, letzter Zugriff: 14.03.2008.

Flamholtz, E. G. (1974): "Human Resource Accounting. A review of Theory and Research." in: Journal of Management Studies 11 (1), S.44-61.
Fleischer, S. M. (1997): Strategische Kooperationen: Planung, Steuerung, Kontrolle. Lohmar, Eul.
Foit, M. (2005): Management operationeller IT-Risiken in Banken. Regensburg, Univ.-Verl Regensburg.
Fontanari, M. L. (1996): Kooperationsgestaltungsprozesse in Theorie und Praxis. Berlin, Duncker & Humblot.
Ford, D. P. (2001): Trust and Knowledge Management: The Seeds of Success. in: Holsapple, C. W. Handbook on Knowledge Management 1. Knowledge Matters. Berlin, Springer, S.553-575.
Foss, N. J. (2005): Strategy, Economic Organization, and the Knowledge Economy. The Coordination of Firms and Resources. Oxford, Oxford Univ. Press.
Fox, D. (2003): "Security-Awareness oder die Wiederentdeckung des Menschen in der IT Sicherheit." in: Datenschutz und Datensicherheit 27 (11), S.676-680.
Fränkl, G., Karpf, P. (2004): Digital Rights Management - Systeme. Einführung, Technologien, Recht, Ökonomie und Marktanalyse. München, PG.
Freeman, E. H. (2004): "Document Theft: Appropriate Responses." in: Edpacs 17 (5), S.1-7.
Fumy, W., Sauerbrey, J. (2005): Identity & Access Management - Schneller ROI und verbesserte Sicherheit durch effiziente Rechtevergabe und Zugriffskontrolle. in: Kuhlin, B.,Thielmann, H. Real-Time Enterprise in der Praxis. Fakten und Ausblick. Berlin, Springer, S.289-305.
Füser, K., Rödel, K., Kang, D. (2002): "Identifizierung und Quantifizierung von Operational Risk." in: Finanz Betrieb 4 (9), S.495-502.
Gabriel, R., Dittmar, C. (2001): "Der Ansatz des Knowledge Managements im Rahmen des Business Intelligence." in: HMD - Praxis der Wirtschaftsinformatik 38 (222), S.17-28.
Gadatsch, A., Uebelacker, H. (2006): "Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte." in: HMD - Praxis der Wirtschaftsinformatik (248), S.44-50.
Gahl, A. (1991): Die Konzeption strategischer Allianzen. Berlin, Duncker & Humblot.
Gaitanides, M., Scholz, R., Vrohlings, A., Raster, M. (1994): Prozeßmanagement: Konzepte, Umsetzungen und Erfahrungen des Reengineering. München, Wien, Carl Hanser Verlag.
Galbraith, J. K. (1969): Die moderne Industriegesellschaft. München, Droemer Knaur.
Ganz, H., Hermann, S. (2000): Vom Umgang mit der Zukunftsressource Wissen. in: Bullinger, H. J.,Hermann, S. Wettbewerbsfaktor Kreativität. Wiesbaden, Gabler, S.111-132.
Garvin, D. A. (1988): Managing quality: the strategic and competitive edge. New York, Free Press.
Garvin, D. A. (1993): " Building a Learning Organization." in: Harvard Business Review 71 (7-8), S.78-91.
Gaudig, S. (2005): Wissensrisiko-Analyse als Ansatz zur Bewertung von Wissensmanagementkonzepten in Unternehmen. in: Jung, R.,Schiller, U. Tagungsband zum Workshop “Potentiale des Informations- und Wissensmanagements“ Arbeitsbericht Nr. 171, Institut für Wirtschaftsinformatik, Universität Bern. S.1-8.
Gebert, H., Kutsch, O. (2003): "Potentiale des Skill-Managements." in: Wirtschaftsinformatik 45 (2), S.227–229.
Geiger, H., Piaz, J.-M. (2001): Identifikation und Bewertung operationeller Risiken. in: Schierenbeck, H., Rolfes, B.,Schüller, S. Handbuch Bankcontrolling. 2.Auflage, Wiesbaden, Gabler.
Gemmerich, M., Stratmann, J. (1998): "Wissensmanagement in der Praxis." in: Technologie & Management 47 (1), S.24-27.
Gerick, T. (2004): "IT-Risiken steuern: Damoklesschwert IT." in: manage it (7-8), S.12-15.
Glazer, R. (1999): "Winning in Smart Markets." in: Sloan Management Review 40 (4), S.59-69.
Gleißner, W. (2001): Identifikation, Messung und Aggregation von Risiken. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.111-137.

Gleißner, W. (2001): Ratschläge für ein leistungsfähiges Risikomanagement - eine Checkliste. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.253-266.

Gleißner, W., Füser, K. (2001): Moderne Frühwarn- und Prognosesysteme für Unternehmensplanung und Risikomanagement. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.175-198.

Gleißner, W., Meier, G. (2001): Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten., Wiesbaden, Gabler.

Gleißner, W., Romeike, F. (2005): Risikomanagement: Umsetzung, Werkzeuge, Risikobewertung; Controlling, Qualitätsmanagement und Balanced Scorecard als Plattform für den Aufbau. Freiburg, Haufe.

Gordon, L. A., Loeb, M. P. (2001): "Using Information Security as a Response to Competitor Analysis System." in: Communications of the ACM 44 (9), S.70-75.

Gordon, L. A., Loeb, M. P. (2006): "Budgeting Process for Information Security Expenditures." in: Communications of the ACM 49 (1), S.121-125.

Gordon, L. A., Loeb, M. P., Sohail, T. (2003): "A Framework for Using Insurance for Cyber-Risk Management." in: Communications of the ACM 46 (3), S.81-85.

Gorrod, M. (2004): Risk Management Systems: Process, Technology and Trends. Basingstoke, Palgrave Macmillan.

Gostev, A. (2007): Malware-Entwicklung im ersten Halbjahr 2007, Analyse durch Kaspersky Lab. URL: http://www.viruslist.com/de/analysis?pubid=200883575, letzter Zugriff: 14.03.2008.

Göttgens, O., Sander, B., Wirtz, B. W., Dunz, M. (2001): BBDO Consulting Arbeitspapier, Markenbewertung als strategischer Erfolgsfaktor, Universität Witten/Herdecke.

Gottwald, R. (1990): Entscheidung unter Unsicherheit: Informationsdefizite und unklare Präferenzen. Wiesbaden, Gabler.

Grant, R. M. (1991): "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation." in: California Management Review 33 (3), S.114-135.

Grant, R. M. (1996a): "Knowledge, Strategy and the Theory of the Firm." in: Strategic Management Journal 17 (12), S.109-122.

Grant, R. M. (1996b): "Prospering in Dynamically-competitive Environments: Organizational Capability as Knowledge Integration." in: Organization Science 7 (4), S.375-387.

Grant, R. M. (1997): "The knowledge-based View of the Firm: Implications for Management Practice." in: Long Range Planning 30 (3), S.450-454.

Grant, R. M. (2001): Contemporary strategy analysis. Malden, Blackwell.

Grant, R. M., Baden-Fuller, C. (1995): "A knowledge-based theory of inter-firm collaboration." in: Academy of Management Journal, S.17-21.

Gronau, N., Uslar, M. (2004): Integrating Knowledge Management and Human Resources via Skill Management. in: Proceedings of I-KNOW ’04, Graz, 30. Juni 30 - 2.Juli 2004, S.135-142.

Gulati, R., Nohira, N., Zaheer, A. (2000): "Strategic Networks." in: Strategic Management Journal 21 (3), S.203-215.

Güldenberg, S. (1997): Wissensmanagement und Wissenscontrolling in lernenden Organisationen: ein systemtheoretischer Ansatz. Wiesbaden, DUV.

Gutjahr, G. (1985): Psychologie des Interviews: In Praxis und Theorie. Heidelberg, Sauer.

Hadden, L. B., Hermanson, D. R. (2003): "Is your audit committee watching IT risks?" in: The Journal of Corporate Accounting & Finance 14 (5), S.35-39.

Hahn, D., Krystek, U. (2000): Früherkennungssysteme und KonTraG. in: Dörner, D., Horvath, P.,Kagermann, H. Praxis des Risikomanagements: Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte. Stuttgart, Schäffer-Poeschel, S.73-97.

Haider, S., Mariotti, F. (2004): Filling knowledge gaps: Knowledge sharing accross interfirm boundaries and occupational communities. in: The Fifth European Conference on Organizational Knowledge, Learning and Capabilities, Innsbruck.

Hain, S. (2007): Wissensschutz - Regelungen und Maßnahmen zum Schutz wettbewerbsrelevanten Wissens am Beispiel ausgewählter Wissensprozesse, Diplomarbeit, Universität Halle.

Hall, B. H., Jaffe, A., Trajtenberg, M. (2000a): Market Value and Patent Citations: A First Look, Working Paper W 17, Universität Oxford.

Hall, H., Jaffe, A., Trajetenberg, M. (2000b): Market value and patent citations - a first look. University of California at Berkley working papers.

Hall, R. (1989): "The Management of Intellectual Assets: A New Corporate Perspective." in: Journal of General Management 15 (1), S. 53-68.

Hall, R. (1992): "The Strategic Analysis of Intangible Resources." in: Strategic Management Journal 13 (2), S.135-144.

Hall, R. (1993): "A framework linking intangible resources and capabilities to sustainable competitive advantage." in: Strategic Management Journal, 14, S.607-618.

Haller, M. (1978): "Risiko-Management, neues Element in der Führung." in: IO: Management-Zeitschrift industrielle Organisation 47 (11), S.483-487.

Haller, M. (1986): Risiko-Management. Eckpunkte eines integrierten Konzeptes. in. Risiko-Management, Schriftenreihe zur Unternehmensführung. Wiesbaden, Gabler.

Hamel, G. (1991): "Competition for Competence and Inter-Partner Learning Within International Strategic Alliances." in: Strategic Management Journal 12 (Summer Special Issue), S.83-103.

Hamel, G., Doz., Y. L., Prahalad, C. K. (1989): "Collaborate with your competitors and win." in: Harvard Business Review 67 (1), S.133-139.

Hamerle, A. (1996): Formelsammlung zur Statistik für Wirtschafts- und Sozialwissenschaftler, Lehrstuhl für Statistik, Universität Regensburg.

Hansen, H. R., Neumann, G. (2005): Wirtschaftsinformatik 1: Grundlagen und Anwendungen. 9.Auflage, Stuttgart, Lucius & Lucius.

Hansen, M., Krasemann, H., Rost, M., Genghini, R. (2003): "Datenschutzaspekte von Identitätsmanagementsystemen." in: DuD Datenschutz und Datensicherheit 27 (9), S.551-555.

Happel, E., Liebewein, P. (2000): Risikofrüherkennung in Versicherungsunternehmen - Aspekte zur Unterstützung des Risk-Managements nach KonTraG, Manuskript 27, München.URL: http://www.inriver.bwl.uni-muenchen.de/forschung/publikationen/Manuskripte/Manuskript_27.pdf, letzter Zugriff: 14.03.2008.

Harrant, H., Hemmrich, A. (2004): Risikomanagement in Projekten. München, Hanser.

Hauri, P., Lecomte, G. (2007): "Umsetzung von Basel II. Herausforderungen und Stolpersteine." in: Der Schweizer Treuhänder (3), S.169-173.

Hawthorn, N. (2002): "Den Wissensschatz im Unternehmensnetz sichern." in: Wissensmanagement - Zeitschrift für Innovation (6), S.45-47.

Heinen, E. (1966): Das Zielsystem der Unternehmung: Grundlagen betriebswirtschaftlicher Entscheidungen. Wiesbaden, Gabler.

Heisig, P., Vorbeck, J. (1998): Benchmarking Wissensmanagement - Best Practices in Deutschland und Europa, Präsentation CUB Konferenz Wissensmanagement in Darmstadt, 17.-18. November.

Helm, R., Mehlhorn, A., Strohmayer, M. (1996): "Die Vertrauensproblematik bei zwischen betrieblichen Kooperationen in der mittelständischen Industrie." in: Zeitschrift für Planung 7, S.73-90.

Helm, R., Meiler, R. C. (2004): Intangible Ressourcen, Zielsystem und Management interner Wissenspotentiale. in: Horváth, P. Intangibles in der Unternehmenssteuerung. Strategien und Instrumente zur Wertsteigerung des immateriellen Kapitals. München, Vahlen, S.387-403.

Helmke, S., Risse, R. (1999): "Chancen- und Risikomanagement im Konzern Deutsche Post AG." in: krp-Kostenrechnungspraxis 43 (5), S.277-283.

Helten, E., Hartung, T. (2002): Instrumente und Modelle zur Bewertung industrieller Risiken. in: Hölscher, R.,Elfgen, R. Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken. Wiesbaden, Gabler, S.255-271.

Henselmann, K. (2001): Das KonTraG und seine Anforderungen an das Risikomanagement. in: Götze, U., Henselmann, K.,Mikus, B. Risikomanagement. Heidelberg, Physica, S.29-46.

Hermann, D. C. (1996): Strategisches Risikomanagement kleiner und mittlerer Unternehmen., Berlin, Köster.

Herwig, V., Schlabitz, L. (2004): "Unternehmensweites Berechtigungsmanagement." in: Wirtschaftsinformatik 46 (4), S.289-294.

Hess, T., Ünlü, V., Faecks, W.-I., Rauchfuß, F. (2004a): "Digitale Rechtemanagement-Systeme. Technische Grundlagen und ökonomische Wirkungen." in: Information Management & Consulting 19 (3), S.53-58.

Hess, T., Ünlü, V., Faecks, W.-I., Rauchfuß, F. (2004b): Rechtemanagement als Lösungsansatz aus dem Digitalen Dilemma, Gemeinsame Studie des Instituts für Wirtschaftsinformatik und Neue Medien und Capgemini.

Hiles, A., Barnes, P. (2001): The Definitive Handbook of Business Continuity Management. Chichester, Wiley.

Hill, R. C., Hellriegel, D. (1994): "Critical contingencies in joint venture management: Some lessons from managers." in: Organization Science 5 (4), S.594-607.

Hillson, D. (1999): Developing Effective Risk Responses. in: Proceedings of the 30th Annual Project Management Institute, Philadelphia.

Hippmann, H.-D. (1997): Statistik für Wirtschafts- und Sozialwissenschaftler. 2.Auflage, Stuttgart, Schäffer-Poeschel.

Hirschmann, P. (1998): Kooperative Gestaltung unternehmensübergreifender Geschäftsprozesse. Wiesbaden, Gabler.

Hirschmann, S., Romeike, F. (2004): "IT Sicherheit als Rating-Faktor." in: RATINGaktuell (01), S.12-18.

Hochstädter, D. (1989): Einführung in die statistische Methodenlehre. 6.Auflage, Frankfurt a. M., Deutsch.

Hofmann, M. (2006): Management operationeller IT-Risiken: im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben. Hamburg, Kovac.

Holm, K. (1986): Die Befragung 1: der Fragebogen - Die Stichprobe. 3.Auflage, Tübingen, Francke.

Holm, S. (1979): "A simple sequentially rejective multiple test procedure." in: Scandinavian Journal of Statistics 6, S.65-70.

Hölscher, R. (1987): Risikokosten-Management in Kreditinstituten: ein integratives Modell zur Messung und ertragsorientierten Steuerung der bankbetrieblichen Erfolgsrisiken. Frankfurt a. M., Knapp.

Hommel, W., Reiser, H. (2005): Federated Identity Management: Die Notwendigkeit zentraler Koordinationsdienste. in: Müller, P., Gotzheim, R.,Schmitt, J. B. Kommunikation in Verteilten Systemen (KiVS): Kurzbeiträge und Workshop der 14. GI/ITG-Fachtagung, 28. Februar bis 3. März 2005. Kaiserslautern, S.65-72.

Hornung, K., Reichmann, T., Diederichs, M. (1999): "Risikomanagement Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen." in: Controlling (7), S.317-325.

Huang, K.-T., Lee, W. Y., Wang, R. Y. (1999): Quality information and knowledge. Upper Saddle River, Prentice-Hall.

Huber, M. (1998): Bewertung von Dienstleistungsunternehmen: das Human Capital als wertbestimmender Faktor in Theorie und Praxis. Bern, Haupt.
Hümmer, B. (2001): Strategisches Management von Kernkompetenzen im Hyperwettbewerb: Operationalisierung kernkompetenzorientierten Managements für dynamische Umfeldbedingungen. Wiesbaden, DUV.
Humpert, F. (2004): "IT Sicherheit." in: HMD - Praxis der Wirtschaftsinformatik 236, S.7-18.
Hunter, L., E., W., Wyatt, A. (2005): Measuring Intangible Capital: A Review of Current Practice,
Husman, T. B. (2001): Efficiency in Inter-Organisational Learning: A Taxonomy of Knowledge Transfer Costs. in: DRUID Winter Conference 2001, Kopenhagen.
Ianella, R. (2002): Open Digital Rights Language (ODRL) Version 1.1. URL: http://www.odrl.net/1.1/ODRL-11.pdf, letzter Zugriff: 14.03.2008.
IDW (1999): "IDW Prüfstandard: Die Prüfung des Risikofrüherkennungssystems nach §317 Abs. 4 HGB (IDW PS 340)." in: Die Wirtschaftsprüfung (16), S.658-662.
IDW (2001): Entwurf IDW Prüfungsstandard: Abschlußprüfung bei Einsatz von Informationstechnologie,
Imboden, C. (1983): Ein entscheidungsbezogenes Risikohandhabungsverfahren. Bern, Haupt.
Inkpen, A. C. (2000): "Learning through joint ventures: A framework of knowledge acquisition." in: Journal of Management Studies 37 (7), S.1019-1043.
Inkpen, A. C., Currall, S. C. (2004): "The Coevolution of Trust, Control, and Learning in Joint Ventures." in: Organization Science 15 (5), S.586–599.
IT-Governance-Institute (2005): CobiT - Control Objectives, Management Guidelines, Maturity Models, Version 4.0,
IT-Research (2003): eProvisioning & Identity Management. Business Value, Markt & Anbieter.
Itami, H. (1987): Mobilizing Invisible Assets. Cambridge, Harvard Univ. Press.
Jacob, M., Ebrahimpur, G. (2001): "Experience vs expertise: The role of implicit understandings of knowledge in determining the nature of knowledge transfer in two companies." in: Journal of Intellectual Capital 2 (1), S.74-88.
Jennex, M. E. (2006): Security and Knowledge Management Success. in: The Second Secure Knowledge Management Workshop (SKM) 2006, Brooklyn.
Johnson, R. A., Wichern, D. W. (1992): Applied multivariate statistical analysis. 3.Auflage, Englewood Cliffs, Prentice-Hall Internat.
Joia, L.-A. (2000): "Measuring intangible corporate assets. Linking business strategy with intellectual capital." in: Journal of Intellectual Capital 1 (1), S.68-84.
Jonen, A. (2005): Semantische Analyse des Risikobegriffs und Bildung eines Begriffskonzeptes für den IT-Dienstleistungsbereich, in: Corsten, H. (Hrsg.) Schriften zum Produktionsmanagement, Nr. 74 Dienstleistungskolloquium am 21.04.2005 an der Universität Kaiserslautern.
Jonen, A., Müller, J. (2006): Risk Evaluator - Roisiko-orientierte Entscheidungsunterstützung bei Investitionen in IT. in: Multikonferenz Wirtschaftsinformatik MKWI 2006, Band 2, Passau, GITO, S.141-154.
Jordan, J., Lowe, J. (2004): "Protecting Strategic Knowledge: Insights from Collaborative Agreements in the Aerospace Sector." in: Technology Analysis and Strategic Management 16 (2), S.241-259.
Jorion, P. (2003): Financial risk manager handbook. 2.Auflage, Hoboken, Wiley.
Jovic, D., Piaz, J.-M. (2001): "Operational Risk Management als kritischer Erfolgsfaktor für Banken." in: Der Schweizer Treuhänder 10 (1), S.923-930.
Junginger, M. (2005): Wertorientierte Steuerung von Risiken im Informationsmanagement. Wiesbaden, DUV.
Junginger, M., Krcmar, H. (2001): IT-Risk-Management - fit für E-Business? in: Buhl, H.-U. Information age economy. Heidelberg, Physica, S.395-408.

Junginger, M., Krcmar, H. (2003): "Risikomanagement im Informationsmanagement - Eine spezifische Aufgabe des IV-Controllings." in: Information Managment & Consulting 18 (2), S.16-23.
Junginger, M., von Balduin, A., Krcmar, H. (2003): "Operational Value at Risk und Management von IT Risiken." in: WISU (03), S.356-364.
Kahn, B. K., Strong, D. M., Wang, R. Y. (2002): "Information Quality Benchmarks: Product and Service Performance." in: Communications of the ACM 45 (4), S.184 -192.
Kale, P., Singh, H., Perlmutter, H. (2000): "Learning and Protection of Proprietary Assets in Strategic Alliances: Building Relational Capital." in: Strategic Management Journal 21 (3), S.217-237.
Kaplan, R. S., Norton, D. P. (1996): The Balanced Scorecard: Translating Strategy into Action. Boston, Harvard Business School Press.
Kaplan, R. S., Norton, D. P. (2004): "Measuring the Strategic Readiness of Intangible Assets." in: Harvard Business Review 82 (2), S. 52-63.
Kaplan, S., Garrick, B. J. (1981): "On the quantitative definition of risk." in: Risk Analysis 1 (1), S.11-27.
Karten, W. (1972): "Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsnehmers - betriebswirtschaftliche Aspekte." in: Zeitschrift für die gesamte Versicherungswirtschaft 61, S.279-299.
Karten, W. (1993): Risk Management. in: Wittmann, W.,Kern, W. Handwörterbuch der Betriebswirtschaft, Teilband 3. 5.Auflage, Stuttgart, Schäffer-Poeschel, S.3813-3824.
Kaufmann, L., Schneider, Y. (2006): Intangible Unternehmenswerte als internationales Forschungsgebiet der Unternehmensführung - Literaturübersicht, Schwerpunkte und Forschungslücken. in: Matzler, K. Immaterielle Vermögenswerte. Handbuch der intangible Assets. Berlin, Schmidt, S.23-41.
Kazmier, L. J. (1999): Wirtschaftsstatistik. 3.Auflage, Frankfurt a. M., McGraw-Hill.
Keitsch, D. (2000): Risikomanagement. Stuttgart, Schäffer-Poeschel.
Keller, H. E. (2004): "Auf sein Auventura und Risigo handeln. Zur Sprach- und Kulturgeschichte des Risiko-Begriffs." in: Risknews 1 (1), S.60-65.
Kendall, R. (1998): Risk Management: Unternehmensrisiken erkennen und bewältigen. Wiesbaden, Gabler.
Kern, M. (2003): Risikomanagement auf der Basis von Corporate Goverance und KonTraG. in: Töpfer, A.,Mehdorn, A. Risikomanagement: vom reaktiven zum präventiven Management von Risiken. Dresden, WGMU, S.33-51.
Kern, P., Braun, M., Zinser, S. (1998): "Erfolgsfaktor Wissensmanagement. Neue Aufgaben für unternehmerisch denkende Technopreneure im Büro der Zukunft." in: M&B 6, S.8-14.
Keßler, H., Winkelhofer, G. A. (2002): Projektmanagement: Leitfaden zur Steuerung und Führung von Projekten. 3.Auflage, Berlin, Springer.
Kiechle, B. (2001): Sonderrisiken, Außergewöhnliche Risiken und ihre Versicherung, Münchener Rückversicherungs-Gesellschaft Bereich Unternehmenskommunikation. München.
Kimball, R. C. (2000): "Failures in Risk Management." in: New England Economic Review 6 (1), S.3-12.
Kirmße, S. (2003): Das Management operationeller Risiken, Präsentation Alpbacher Bankenseminar.
Klett, G. (1993): "Risiko-Analyse mit Fuzzy-Logik." in: KES Zeitschrift für Kommunikations- und EDV-Sicherheit 9 (6), S.28-32.
Klingler, U., Räss-Fernandez, A., Catellani, B. (2004): "Mitarbeiter sind der Grund für Erfolg." in: KMU Magazin (10), S.1-7.
Klomfass, M., Quadt, R. (2001): "Einbettung von Betriebsrisiken in die unternehmensweite Risikosteuerung." in: Betriebswirtschaftliche Blätter (07), S.322-326.
Knaese, B. (1996): Kernkompetenzen im strategischen Management von Banken: der "Resource- based-view" in Kreditinstituten. Wiesbaden, Gabler.

Knaese, B. (2004): Das Management von Know-how-Risiken: eine Analyse von Wissensverlusten im Investment Banking einer Großbank. Wiesbaden, DUV.

Knaese, B., Probst, G. (2001): "Wissensorientiertes Management der Mitarbeiterfluktuation. Eine Methode zur Reduzierung personeller Wissensrisiken." in: zfo Zeitschrift für Führung und Organisation 70 (1), S.35-41.

Knight, F. H. (1921): Risk, Uncertainty and Profit. Boston, Houghton Mifflin.

Knight, S., Burn, J. (2005): "Developing a Framework for Assessing Information Quality on the World Wide Web." in: Informing Science Journal 8, S.159-172.

Know-Center (2006): Jahresbericht 2005, Graz.

Kobi, J. M. (1999): Personalrisikomanagement: eine neue Dimension im Human Resources Management; Strategien zur Steigerung des People Value. Wiesbaden, Gabler.

Kobi, J. M. (2003): Personalrisiken systematisch angehen. in: Schmeisser, W. Internationales Personalcontrolling und internationale Personalinformationssysteme. München, Hampp, S.99-109.

Koch, R. (2005): Versicherbarkeit von IT-Risiken: in der Sach-, Vertrauensschaden- und Haftpflichtversicherung. Berlin, Schmidt.

Kogut, B., Zander, U. (1992): "Knoweldge of the firm, combinative capabilities, and the replication of technology." in: Organization Science 3 (3), S.383-397.

Koller, H., Hentschel, M. (2006): Die Bewertung von Intellectual Property Rights - Verfahren, Anwendung, Eignung und ihre Konsequenzen für die Bewertung von intangible Assets. in: Matzler, K. Immaterielle Vermögenswerte. Handbuch der intangible Assets. Berlin, Schmidt, S.299-329.

Königer, P., Reithmayer, W. (1998): Management unstrukturierter Informationen: wie Unternehmen die Informationsflut beherrschen können. Frankfurt a. M., Campus.

Konrad-Group (1989): The Invisible Balance Sheet. Malmö.

Kontio, J. (2001): Software Engineering Risk Management, A Method, Improvement Framework, and Empirical Evaluation, Dissertation, Universität Helsinki. Helsinki.

KPMG (1998): Integriertes Risikomanagement, Berlin.

KPMG (2003): Basel II - A Closer Look: Managing Operational Risk, URL: http://www.kpmg.ca/en/industries/fs/banking/documents/Basel%20II_%20A%20closer%20look_%20managing%20operational%20risk.pdf, letzter Zugriff: 14.03.2008.

Kraft, G. (2006): Wissensbilanz - Voraussetzung für den Dienstleistungsexport. in: IHK-Stuttgart. Export von Dienstleistungen: Potentiale und Strategien beim "Going international". Stuttgart.

Krämer, G. (2002a): "Das qualitative materielle Risiko bei betriebswirtschaftlichen Entscheidungen." in: Der Steuerberater (6), S.270-273.

Krämer, G. (2002b): "Die Rahmenbedingungen des unternehmerischen Entscheidungsprozess." in: Der Steuerberater (4), S.140-144.

Kratzheller, J. B. (1997): Risiko und Risk Management aus organisationswissenschaftlicher Perspektive. Wiesbaden, DUV.

Kratzke, N. (2006): "Modell-basierte Identifikation interorganisationaler Wissensflüsse." in: Informatik - Forschung und Entwicklung 20 (4), S.196-208.

Krcmar, H. (2005): Informationsmanagement. 4.Auflage, Berlin, Springer.

Krcmar, H., Junginger, M. (2003): Risikomanagement im Informationsmanagement - Herausforderung Collaborative Commerce. in: Kemper, H.-G. Informationsmanagement: neue Herausforderungen in Zeiten des E-Business; Festschrift für Prof. Dr. Dietrich Seibt anlässlich seines 65. Geburtstages. 245-269.Auflage, Lohmar, Eul.

Kreft, H. D. (2004): " Vom Wert des Wissens – Wie lässt sich das intellektuelle Kapital messen und bewerten?" in: Wissensmanagement - Zeitschrift für Innovation 6 (4), S.22-24.

Kremers, M. (2002): Risikoübernahme in Industrieunternehmen: der Value-at-Risk als Steuerungsgröße für das industrielle Risikomanagement, dargestellt am Beispiel des Investitionsrisikos. Sternenfels, Verl. Wiss. und Praxis.

Kronen, J. (1994): Computergestützte Unternehmenskooperation. Potentiale - Strategien - Planungsmodelle. Wiesbaden, DUV.

Kruschwitz, L. (1980): "Bemerkungen zur Risikoanalyse aus theoretischer Sicht." in: Zeitschrift für Betriebswirtschaft 50, S.800-808.

Kruth, W. (2004): IT-Grundlagenwissen: Kompaktwissen Informationstechnik für Datenschutz- und Security-Management. Frechen, Datakontext.

Kubitscheck, V. (2000): "Risk management: finding the value within." in: Balance Sheet 9 (5), S.38-41.

Kuhn, L. (2002): Risikophasenmodell für Operationelle Risiken im Kontext der Gesamtbanksteuerung. in: Eller, R., Gruber, W.,Reif, M. Handbuch Operationelle Risiken: aufsichtsrechtliche Anforderungen, Quantifizierung und Management, Praxisbeispiele. Stuttgart, Schäffer-Poeschel, S.153-178.

Kuppinger, M. (2005): "Identity Management - Basis für sichere Geschäftsprozesse." in: Objektspektrum (1), S.1-4.

Küting, K., Dürr, U. (2003): "Intangibles in der deutschen Bilanzierungspraxis." in: StuB Steuer und Bilanzpraxis (1), S.1-5.

Kütz, M. (2003): Kennzahlen in der IT. Werkzeuge für Controlling und Management. Heidelberg, dpunkt.

Lam, W., Chua, A. (2005): "The mismanagement of knowledge management." in: Aslib Proceedings 57 (5), S.424-433.

Lane, P. J., Salk, J. E., Lyles, M. A. (2001): "Absorptive capacity, learning, and performance in international joint ventures." in: Strategic Management Journal 22 (12), S.1139-1161.

Lanfermann, G., Maul, S. (2002): "Auswirkungen des Sarbanes-Oxley Acts in Deutschland." in: Der Betrieb 55 (34), S.1725-1732.

Lang, J. C. (2004): "Social context and social capital as enablers of knowledge integration." in: Journal of Knowledge Management 8 (3), S.89-105.

Langer, W. (1999): Praktische Durchführung der explorativen Faktorenanalyse, Vorlesungsskript an der Universität Halle-Wittenberg, URL: http://www.soziologie.uni-halle.de/langer/lisrel/index.html, letzter Zugriff: 14.03.2008.

Larsson, R., Bengtsson, L., Henriksson, K., Sparks, J. (1998): "The Interorganizational Learning Dilemma: Collective Knowledge Development in Strategic Alliances." in: Organization Science 9 (3), S.285-304.

Lave, J. (1993): The Practice of Learning. in: Chaiklin, S.,Lave, J. Understanding Practice: Perspectives on Activity and Context. Cambridge, S.3-32.

Learned, E. P., Christensen, C. R., Andrews, K. R., Guth, W. D. (1965): Business Policy. Text and Cases. Homewood, Irwin.

Lee, A. (2005): Intellectual property. in: Reuvid, J. Managing business risk: a practical guide to protecting your business. 2.Auflage, London, Kogan Page, S.155-160.

Lee, J. B., Rosenbaum, A. D. (2003): "Knowledge management: Portal for corporate espionage? Part 1." in: KM World 12 (10).

Lee, Y. W., Strong, D. M., Kahn, B. K., Wang, R. Y. (2002): "AIMQ: a methodology for information quality assessment." in: Information & Management 40 (2), S.133-146.

Lehmann, L. (2002): Patentfibel: von der Idee bis zum Patent. Hannover, Grütter.

Lehner, F. (2000): Organisational Memory: Konzepte und Systeme für das organisatorische Lernen und das Wissensmanagement. München, Hanser.

Lehner, F., Hildebrand, K., Maier, R. (1995): Wirtschaftsinformatik: theoretische Grundlagen. München, Hanser.

Lei, D. (1993): "Offensive and Defensive Uses of Alliances." in: Long Range Planning 26 (4), S.32-41.

Leidinger, B. J. G. (2002): Risikoidentifikation und Maßnahmensteuerung im Rahmen des operativen Risikomanagements. in: Hölscher, R.,Elfgen, R. Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken. Wiesbaden, Gabler, S.239-254.

Leitner, K.-H. (2003): "Wissensbilanzierung. Ein neues Berichtswesen für Forschungsorganisationen und Hochschulen." in: Wissenschaftsmanagement 2 (3/4), S.20-24.

Lesch, T., Richter, A. (2000): "Prävention und Versicherung für Gefahren aus dem Internet." in: Versicherungswirtschaft 55, S.1774-1778 (Teil 1771) und 1856-1856 (Teil 1772).

Lev, B. (2001): Intangibles: Management, Measurement, and Reporting. Washington D.C., Brookings Institution Press.

Lev, B. (2004a): Intangibles at a Crossroads. in: Horváth, P. Intangibles in der Unternehmenssteuerung Strategien und Instrumente zur Wertsteigerung des immateriellen Kapitals. München, Vahlen, S.3-14.

Lev, B. (2004b): "Sharpening the Intangibles Edge." in: Harvard Business Review 82 (6), S.109-116.

Lev, B. (2005): Intangible Assets: Concepts and Measurement. in: Kempf-Leonard, K. Encyclopedia of Social Measurement Vol. 2. Amsterdam, Elsevier, S.299-305.

Licari, J. (2005): "Securing the Information Workplace: Managing Threats to Enterprise E-Mail, IM, and Document Sharing Environments." in: Information Systems Security (Sept.-Okt.), S.45-50.

Liebeskind, J. P. (1997): "Keeping Organizational Secrets: Institutional Protective Mechanisms and Their Costs." in: Industrial and Corporate Change, 6 (3), S.623-663.

Liebowitz, J., Suen, Y. S. (2000): "Developing knowledge management metrics for measuring intellectual capital." in: Journal of Intellectual Capital 1 (1), S.54-67.

Lienert, G. A. (1969): Testaufbau und Testanalyse. Weinheim, Beltz.

Liman, B. (1999): Bewertung des irregulären Verlustes von Know-how: Schäden durch Wirtschaftsspionage und Fluktuation. Köln, Wirtschaftsverlag Bachem.

Lindstaedt, S., Koller, S., Krämer, T. (2004): Eine Wissensinfrastruktur für Projektrisikomanagement - Identifikation und Management von Wissensrisiken. in: Tagungsband zur KnowTech 2004, 6. Konferenz zum Einsatz von Knowledge Management in Wirtschaft und Verwaltung, S. 367-375, München.

Locher, C. (2004): "Management operationeller Risiken - Ein Branchenvergleich." in: BIT 3 (3), S.9-20.

Locher, C., Mehlau, J. I., Hackenberg, R. G., Wild, O. (2004): Risikomanagement in Finanzwirtschaft und Industrie. Eine Analyse des Managements von operationellen Risiken in deutschen Industrie- und Dienstleistungsunternehmen, ibi Research Universität Regensburg.

Loebbecke, C., van Fenema, P. C., Powell, P. (1999): "Co-Opetition and Knowledge Transfer." in: The DATA BASE for Advances in Information Systems 30 (2), S.14-25.

Loomans, D. (2004): "Information RiskScorecard macht Unsicherheitskosten transparent." in: HMD 40 (236), S.43-51.

Lorange, P., Roos, J. (1992): Stolpersteine beim Management Strategischer Allianzen. in: Bronder, C.,Pritzl, R. Wegweiser für Strategische Allianzen. Meilen- und Stolpersteine bei Kooperationen. Frankfurt a. M., Frankfurter Allgemeine Zeitung.

Lubich, H. P. (2006): "IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen." in: HMD - Praxis der Wirtschaftsinformatik (248), S.6-15.

Lucas, L. M. (2005): "The impact of trust and reputation on the transfer of best practices." in: Journal of Knowledge Management 9 (4), S.87-101.

Lück, W. (1998): "Elemente eines Risiko-Managementsystems - Die Notwendigkeit eines Risiko-Managementsystems durch den Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unter- nehmensbereich (KonTraG)." in: Der Betrieb 51 (1/2), S.8-14.

Lück, W., Henke, M., Gaenslen, P. (2002): Die Interne Revision und das Interne Überwachungssystem vor dem Hintergrund eines integrierten Risikomanagements. in: Hölscher, R.,Elfgen, R. Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken. Wiesbaden, Gabler, S.225-238.

Lück, W., Schulte, A. (1997): "Integrierte Materialwirtschaft, Entwicklungstendenzen der Materialwirtschaft in der Brauwirtschaft, Teil III: Kooperationen und Lagerung." in: Brauwelt 137 (17), S.666-671.

Luhmann, N. (1991): Soziologie des Risikos. Berlin, de Gruyter.

Luthy, D. H. (1998): Intellectual capital and its measurement, URL: http://www3.bus.osaka-cu.ac.jp/apira98/archives/htmls/25.htm, letzter Zugriff: 14.03.2008.

Lux, C., Peske, T. (2002): Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie. Wiesbaden, Gabler.

Lyles, M. A., Szabo, K., Kocsis, E., Barden, J., Dhanaraj, C., Steensma, K., Tihanyi, L. (2002): A longitudinal study of organizational learning, unlearning, and innovation among IJVs in a transitional economy. in: Chakravarthy, B., Müller-Stewens, G., Lorange, P.,Lechner, C. Strategy Process: Shaping the Contours of the Field. Oxford, Blackwell, S.191-207.

Machlup, F. (1980): Knowledge: Its Creation, Distribution, and Economic Significance. Princeton University Press.

Mahnke, V. (1999): The Economies of Knowledge-Sharing: Production- and Organization Cost Considerations. in: DRUID Winter Conference 1999, Aalborg, S.1-28.

Maier, E. (1992): Der Schutz des "kritischen" Know-how vor Industriespionage. Idstein, Schulz-Kirchner.

Maier, R. (2004): Knowledge Management Systems: information and communication technologies for knowledge management. 2.Auflage, Berlin, Springer.

Maier, R., Bayer, F. (2005): "IT gestütztes Erfahrungsmanagement im Formenbau." in: WISU Das Wirtschaftsstudium 34 (5), S.675-678.

Maier, R., Hädrich, T., Peinl, R. (2005): Enterprise knowledge infrastructures. Berlin, Springer.

Maier, R., Schmidt, A. (2007): Characterizing Knowledge Maturing: A Conceptual Process Model for Integrating E-Learning and Knowledge Management, 4th Conference Professional Knowledge Management - Experiences and Visions (WM '07), Workshop on Convergence of E-Learning and Knowledge Management, Potsdam, S.325-334.

Mansfield, E. (1985): "How Rapidly Does New Industrial Technology Leak Out?" in: Journal of Industrial Economics 34 (2), S.217-224.

Manthei, K., Schmidt, E. (2005): IT-Sicherheit in Unternehmen. in: Duve, B. Jenseits der Technik: Arbeit im E-Business in kleinen und mittleren Unternehmen. Münster, LIT, S.73-85.

Mantwill, G. J. (1995): "Nutzers Not und Pflichten - Zur Qualität von Informationsdiensten." in: Cogito 11 (3), S.45-49.

Marr, B. (2004): Mapping the dynamics of how Intangibles Create Value. in: Proceedings of the IC Congress, Hanken Business School Helsinki, S.1-13.

Marr, B., Gray, D. (2004): The Three Reasons why Organizations Measure Their Intellectual Capital. in: Horváth, P.,Möller, K. Intangibles in der Unternehmenssteuerung. München, Vahlen, S.99-126.

Marr, B., Schiuma, G., Neely, A. (2004): "Intellectual capital - defining key performance indicators for organizational knowledge assets." in: Business Process Management Journal 10 (5), S.551-569.

Marsh, S. J., Ranft, A. L. (1999): Why Resources Matter: An Empirical Study of the Influence of Knowledge-Based Resources on New Market Entry, in. in: Hitt, M. A. Dynamic Strategic Resources: Development, Diffusion, and Integration. West Sussex, Wiley, S.43-66.

Marsland, V. (2003): Intellectual property. in: Jolly, A. Managing business risk. London, Kogan Page, S.161-167.

Maskus, K. E. (2003): Intellectual property protection: is it being taken too far? in: Curtis, J. M.,Ciuriak, D. Trade policy research, Minister of Public Works and Goverment Services. Ottawa, S.185-198.

Matousek, M., Schlienger, T., Teufel, S. (2004): " Metriken und Konzepte zur Messung der Informationssicherheit." in: HMD - Praxis der Wirtschaftsinformatik 236 (4), S.33-41.

Matusik, S. F. (2002a): "An empirical investigation of firm public and private knowledge." in: Strategic Management Journal 23 (5), S. 457-467.

Matusik, S. F. (2002b): Managing Public and Private Firm Knowledge Within the Context of Flexible Firm Boundaries. in: Choo, C. W.,Bontis, N. The Strategic Management of Intellectual Capital. Oxford, Oxford Univ. Press, S.605-617.

Matusik, S. F., Hill, C. W. (1998): "The utilization of contingent work, knowledge creation, and competitive advantage." in: Academy of Management Review 23 (4), S.680-697.

Mayer, R. C., Davis, J. H., Schoorman, F. D. (1995): "An integration model of organizational trust." in: Academy of Management Review 20 (3), S.709-734.

McGonagle, J., Vella, C. M. (2004): Protecting Your Company from Web-based Competitive Intelligence. in: Vibert, C. Competitive Intelligence: A Framework for Web-Based Analysis and Decision Making. Mason, Thomson, S.69-82.

McGonagle, J. J., Vella, C. M. (1994): Outsmarting: wie man der Konkurrenz ganz legal in die Karten schaut. Stuttgart, Schäffer-Poeschel.

Mehr, R. I., Hedges, B. A. (1974): Risk management: concepts and applications. Homewood, Irwin.

Meier, G. (2001): Markt und Trends im Risk-Management. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.17-26.

Meissinger, J. (2006): Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland. Hamburg, Kovač.

Mentzas, G., Apostolou, D., Young, R. (2003): Knowledge asset management: beyond the process-centred and product-centred approaches. London, Springer.

Menzies, C. (2004): Sarbanes-Oxley Act: professionelles Management interner Kontrollen. Stuttgart, Schäffer-Poeschel.

Merbecks, A. (1995): Zur Organisation des Risikomanagements in Kreditinstituten, Hochschulschrift der Universität Bochum. Bochum.

Mertins, K., Alwert, K. (2003): "Integrierte Wissensbewertung. Ein Instrument zur Bewertung, Steuerung und Bilanzierung von Wissen." in: Zeitschrift für wirtschaftlichen Fabrikbetrieb 11, S.578-582.

Mertins, K., Alwert, K., Will, K. (2006): Measuring Intellectual Capital in European SME. in: 6th International Conference on Knowledge Management (I-Know), Graz, 6.-8. September 2006, S.21-25.

Mertins, K., Heisig, P., Vorbeck, J. (2001): Knowledge Management. Best Practices in Europe. Berlin, Springer.

Mikus, B. (2001): Risiken und Risikomanagement - ein Überblick. in: Götze, U., Henselmann, K.,Mikus, B. Risikomanagement. Heidelberg, Physika, S.3-29.

Mitchell, W., Dussauge, P., Garrett, B. (2002): Alliances With Competitors: How to Combine and Protect Key Resources? in: EURAM 2002, Stockholm.

Mock, R. (2003): "Risiko, Sicherheit und Zuverlässigkeit: Analysemethoden in der „Information and Communication Technology“?" in: Informatik-Spektrum 26 (3), S.167-172.

Mohamed, S., Mynors, D., Grantham, A., Walsh, K., Chan, P. (2006): Understanding One Aspect of the Knowledge Leakage Concept: People. in: European and Mediterranean Conference on Information Systems (EMCIS), 6.-7. Juli 2006, Alicante.

Mohr, J. J., Sengupta, S. (2002): "Managing the paradox of inter-firm learning: the role of governance mechanisms." in: Journal of Business & Industrial Marketing 17 (4), S.292-301.

Möller, K. (2004): Intangibles als Werttreiber. in: Horváth, P. Intangibles in der Unternehmenssteuerung Strategien und Instrumente zur Wertsteigerung des immateriellen Kapitals. München, Vahlen, S.483-495.

Möller, K. (2005): "Erfassung und Bewertung von Intangibles." in: Wissensmanagement - Zeitschrift für Innovation 7 (3), S.4-5.

Mosch, K. (2005): "Wissensbilanzen." in: Wissenschaftsmanagement 7 (3), S.2-3.

Moser, T. (2005): Steuerungsinstrumente und Maßnahmen für Wissensrisiken. Theoretische Untersuchung, Entwurf eines Modells und Entwicklung eines Prototyps. Diplomarbeit an der TU Graz.

Mosiek, T. (2003): "Risiko-Reporting - konzeptionelle und dv-technische Anforderungen an ein Risikoberichtswesen." in: Zeitschrift für Controlling & Management 47 (1), S.15-18.

Mott, B. P. (2001): Organisatorische Gestaltung von Risiko-Managementsystemen. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.199-232.

Mouritsen, J., Bukh, P. N., Marr, B. (2004): "Reporting on intellectual capital: why, what and how?" in: Measuring Business Intelligence 8 (1), S.46-54.

Mourtisen, J. (2005): Intellectual Capital and the management control of knowledge resources. in: Berry, A. J., Broadbent, J.,Otley, D. Management control: theories, issues, and performance. Houndmills, Palgrave Macmillan, S.205-229.

Müller-Stewens, G., Lechner, C. (2005): Strategisches Management: wie strategische Initiativen zum Wandel führen; der St. Galler General Management Navigator. Stuttgart, Schäffer-Poeschel.

Müller-Stewens, G., Osterloh, M. (1996): "Kooperationsinvestitionen besser nutzen: Interorganisationales Lernen als Know-how-Transfer oder Kontext-Transfer?" in: zfo Zeitschrift für Führung und Organisation (1), S.18-23.

Müller-Stingl, A., Neumann, R. (2006): Ausgewählte Methoden zur Bewertung von intangible Assets: Entwicklung eines Business Excellence Navigators. in: Matzler, K. Immaterielle Vermögenswerte. Handbuch der intangible Assets. Berlin, Schmidt, S.43-63.

Müller, C. (2006): Wissen, intangible Assets oder intellektuelles Kapital - eine Begriffswelt in Diskussion. in: Matzler, K. Immaterielle Vermögenswerte. Handbuch der intangible Assets. Berlin, Schmidt, S.3-22.

Müller, W. (1993): Risiko und Ungewissheit. in: Wittmann, W. Handwörterbuch der Betriebswirtschaft, Teilband 3: R - Z. Stuttgart, Poeschel, S.3813-3824.

Mundy, D., Chadwick, D. W. (2004): Secure Knowledge Management for Health Care Organizations. in: Wickramasinghe, N., Gupta, J. N. D.,Sharma, S. K. Creating knowledge-based healthcare organizations. Hershey, Idea Group, S.321-337.

Müßig, S. (2006): "Haben Sicherheitsinvestitionen eine Rendite?" in: HMD - Praxis der Wirtschaftsinformatik (248), S.35-43.

Nagel, C. (2006): Von der Wissenbilanz zur Wissensbewertung: das Knowledge-Asset-Measurement-System. in: Streich, D. Moderne Dienstleistungen: Impulse für Innovation, Wachstum und Beschäftigung; Beiträge der 6. Dienstleistungstagung des BMBF. Frankfurt a. M., Campus, S.477-484.

Naumann, F., Rolker, C. (2000): Assessment Methods for Information Quality Criteria, in: 5th Conference on Information Quality, Cambridge. S.148-162.
Nemetz, M. (2006): Towards a Model for Creating Comparable Intellectual Capital Reports. in: 6th International conference on Knowlededge Management (I-Know '06), Graz, 6.-8. September 2006, S.13-20.
Nettesheim, C., Grebe, M., Kottmann, D. (2003): "Business Process Outsourcing - aber richtig!" in: Information Management & Consulting (18), S.24-30.
Neumann, R. (1995): Risiko Organisation - organisiertes Risiko: Beiträge zur integrativ-systemorientierten Verarbeitung selbsterzeugter Risikopotentiale in und von Organisationen. Frankfurt a. M., Lang.
Neus, A. (2003): Evolving Knowledge: Empowering Information Users, in: Proceedings of the Eigth Conference on Information Quality (ICIQ). S.41-50.
Nicklisch, H. (1912): Allgemeine kaufmännische Betriebswirtschaftslehre als Privatwirtschaftslehre des Handels (und der Industrie). Leipzig, Poeschel.
Niedermeier, R., Huth, A. A. (2006): Rechtlicher Leitfaden Lauschabwehr und Informationsschutz,
Nielsen, B. (2002): "Synergies in Strategic Alliances: Motivation and Outcomes of Complementary and Synergistic Knowledge Networks." in: Journal of Knowledge Management Practice 3.
Nieto, M., Pérez-Cano, C. (2004): "The Influence of Knowledge Attributes on Innovation Protection Mechanisms." in: Journal of Knowledge and Process Management 11 (2), S.117-126.
Nohr, H. (2001): Management der Informationsqualität. Arbeitspapiere Wissensmanagement Nr.3/2001, Stuttgart.
Nonaka, I. (1991): "The Knowledge-Creating Company." in: Harvard Business Review 69 (11-12), S.96-104.
Nonaka, I., Takeuchi, H. (1995): The Knowledge-Creating Company: how Japanese Companies create the Dynamics of Innovation. New York, Oxford Univ. Press.
Nonaka, I., Toyama, R., Konno, N. (2000): "SECI, ba, and leadership: a unified model of dynamic knowledge creation." in: Long Range Planning 33 (1), S.5-34.
Nooteboom, B., Berger, H., Noorderhaven, N. G. (1997): "Effects of Trust and Governance on Relational Risk." in: Academy of Management Journal 40 (2), S.308-338.
Norman, P. M. (2001): "Are your secrets safe? Knowledge protection in strategic alliances." in: Business Horizons 44 (6), S.51-60.
Norman, P. M. (2002): "Protecting knowledge in strategic alliances - resource and relational characteristics." in: Journal of High Technology Management Research 13 (2), S.177-202.
Norman, P. M. (2004): "Knowledge acquisition, knowledge loss, and satisfaction in high technology alliances." in: Journal of Business Research 57 (6), S.610-619.
Norrman, A., Lindroth, R. (2004): Categorization of Supply Chain Risk and Risk Management. in: Brindley, C. Supply chain risk. Aldershot, Ashgate, S.14-27.
North, K. (1999): Wissensorientierte Unternehmensführung: Wertschöpfung durch Wissen. 2.Auflage, Wiesbaden, Gabler.
North, K., Probst, G., Romhardt, K. (1998): "Wissen messen - Ansätze, Erfahrungen und kritische Fragen." in: zfo Zeitschrift für Führung und Organisation 67 (3), S.158-166.
Nosek, J. T. (2006): KM needs SAFE Docs™ - Secure Access for Essential Documents. in: The Second Secure Knowledge Management Workshop (SKM) 2006, Brooklyn.
Noufal, P. P. (2003): Information Technology- Misuse and Abuse. in: Bavakutty, M. Information access, management and exchange in the technological age. New Delhi, Ess Ess Publications, S.140-149.
Oberparleiter, K. (1930): Funktionen- und Risikenlehre des Warenhandels. Berlin, Spaeth & Linde.
Oberschulte, H. (1996): Organisatorische Intelligenz - Ein Vorschlag zur Konzeptdifferenzierung. in: Schreyögg, G.,Conrad, P. Managementforschung Band 6. Berlin, de Gruyter.

Oehler, A., Unser, M. (2002): Finanzwirtschaftliches Risikomanagement. Berlin, Springer.
Oepping, H., Siemes, A. (2003): "Strategisches Risikomanagement mit der Balanced Scorecard." in: Controller Magazin 3 (3), S.229-238.
Oliver, A. L. (2004): "On the duality of competition and collaboration: network-based knowledge relations in the biotechnology industry." in: Scandinavian Journal of Management 20 (1-2), S.151-171.
Oxley, J. E., Sampson, R. C. (2004): "The Scope and Governance of International R&D Alliances." in: Strategic Management Journal 25 (8-9), S.723-749.
Paik, Y. (2005): "Risk Management of Strategic Alliances and Acquisitions between Western MNCs and Companies in Central Europe." in: Thunderbird International Business Review 47 (4), S.489-511.
Parise, S., Henderson, J. C. (2001): "Knowledge resource exchange in strategic alliances." in: IBM Systems Journal 40 (4), S.908-924.
Paulus, S. (2000): Risiken beim Einsatz von Informationstechnologie. in: Dörner, D., Horvath, P.,Kagermann, H. Praxis des Risikomanagements: Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte. Stuttgart, Schäffer-Poeschel, S.379-413.
Pedersen, T., Petersen, B., Sharma, D. (2003): "Knowledge Transfer Performance of Multinational Companies." in: Management International Review 43 (Special Issue), S.69-90.
Peltier, T. R. (2001): Information security risk analysis. 1.Auflage, Boca Raton, Auerbach.
Peltier, T. R. (2005): Information security risk analysis. 2.Auflage, Boca Raton, Auerbach.
Peltier, T. R. (2006): "Social Engineering: Concepts and Solutions." in: EDPACS 18 (8), S.1-12.
Penrose, E. T. (1959): The Theory of the Growth of the Firm. New York, Wiley.
Persch, P.-R. (2003): Die Bewertung von Humankapital. in: Rasche, C.,Wagner, D. Professional Services: Mismanaged Industries - Chancen und Risiken. München, Hampp, S.323-342.
Peter, C. F. (2002): Unternehmerisches Risikomanagement: Konsequenzen einer integrierten Risikobewältigung für die Versicherung. St. Gallen, IVW.
Peter, J. P. (1979): "Reliability: A Review of Psychometric Basis and Recent Marketing Practices." in: Journal of Marketing Research 16 (2), S.6-17.
Peteraf, M. A. (1993): "The Cornerstones of Competitive Advantage: A Resource-based View." in: Strategic Management Journal 14, S.179-192.
Petralia, A. (2005): "Identity Management." in: Notitia (9), S.9-11.
Pfeiffer, W. (1965): Absatzpolitik bei Investitionsgütern der Einzelfertigung: Möglichkeiten und Grenzen des Einsatzes absatzpolitischer Instrumente im Sondermaschinenbau. Stuttgart, Poeschel.
Pfitzer, N., Füser, K., Meireis, K., Wulfkühler, S. (2002): "Risikomanagement in der WP-Gesellschaft." in: Der Betrieb 39, S.2005-2009.
Piaz, J.-M. (2002): Operational Risk Management bei Banken. Zürich, Versus.
Piber, M. (2004): Messen und Managen von Intangibles in unterschiedlichen organisationalen Kontexten. in: Horváth, P. Intangibles in der Unternehmenssteuerung Strategien und Instrumente zur Wertsteigerung des immateriellen Kapitals. München, Vahlen, S.497-517.
Picot, G. (2001): Überblick über die Kontrollmechanismen im Unternehmen nach KonTraG. in: Lange, K. W. Risikomanagement nach dem KonTraG: Aufgaben und Chancen aus betriebswirtschaftlicher und juristischer Sicht. München, Vahlen, S.5-37.
Pohlmann, N. (2006): "Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?" in: HMD - Praxis der Wirtschaftsinformatik (248), S.26-34.
Polanyi, M. (1958): Personal knowledge: towards a post-critical philosophy. Chicago, Univ. of Chicago Press.
Polanyi, M. (1966): The Tacit Dimension. London, Doubleday & Company.

Porter, M. E. (1980): Competitve Strategy: Techniques for Analyzing Industries and Competitors. New York, Free Press.
Porter, M. E. (1981): "The contribution of industrial organization to strategic management." in: Academy of Management Review 6, S.609-620.
Porter, M. E. (1985): Competitive Advantage. Creating and Sustaining Superior. New York, Free Press.
Porter, M. E. (1989): Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten. Frankfurt a. M., Campus.
Porter, M. E. (1990): The Competitive Advantage of Nations. London, Macmillan.
Prahalad, C. K., Hamel, G. (1990): "The Core Competence of the Corporation." in: Harvard Business Review 68 (5-6), S.79-91.
PricewaterhouseCoopers (2006): Information Security Breaches Survey 2006, http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16.
Probst, G., Knaese, B. (1998): Risikofaktor Wissen: wie Banken sich vor Wissensverlusten schützen. Wiesbaden, Gabler.
Probst, G., Knaese, B. (1999): "Risiko von Wissensverlusten als Folge von Mergers & Acquisitions." in: Manager Bilanz 3 (4), S.11-15.
Probst, G., Raub, S., Romhardt, K. (1998): Wissen managen: Wie Unternehmen ihre wertvollste Ressource optimal nutzen. 2.Auflage, Wiesbaden, Gabler.
Probst, G., Raub, S., Romhardt, K. (2006): Wissen managen: wie Unternehmen ihre wertvollste Ressource optimal nutzen. 5.Auflage, Wiesbaden, Gabler.
Probst, G. J. B., Arne Deussen, A., Eppler, M. J., Raub, S. P. (2000): Kompetenz-Management: wie Individuen und Organisationen Kompetenz entwickeln. Wiesbaden, Gabler.
Prokein, O. (2005): Management von Sicherheitsrisiken bei Banken. in: Doctoral Consortium auf der WI 2005.
PWC (2001): Risikomanagement bei Kapitalgesellschaften - ein ganzheitlicher Ansatz. URL: http://www.pwc.com/de/ger/ins-sol/publ/RM_bei_KAGen.pdf, letzter Zugriff: 14.03.2008.
PWC (2003): Immaterielle Werte und andere weiche Faktoren in der Unternehmensberichterstattung, Industriestudie.
Queensland (2001): Queensland Government, Best Practice Guide Information Risk Management. URL: http://www.governmentict.qld.gov.au/02_infostand/downloads/riskmanagementbpg.pdf, letzter Zugriff: 14.03.2008.
Rada, R. (2000): Consensus versus speed. in: Jakobs, K. Information Technology Standards and Standardization: A Global Perspective. Idea Group, New York, S.19 - 34.
Rannenberg, K. (2000): "Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet." in: Wirtschaftsinformatik 42, S.489-497.
Raub, S., Büchel, B. (1996): "Organisationales Lernen und Unternehmensstrategie - »core capabilities« als Ziel und Resultat organisationalen Lernens." in: Zeitschrift Führung und Organisation 65 (1), S.26-31.
Reed, R., DeFillippi, R. J. (1990): "Causal Ambiguity, Barriers to Imitation, and Sustainable Competitive Advantage." in: Academy of Management Review 15, S.88-102.
Reh, G. (2001): Ablaufplan: Einführung eines Risiko-Managementsystems. in: Gleißner, W.,Meier, G. Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten. Wiesbaden, Gabler, S.27-40.
Rehäuser, J., Krcmar, H. (1996): Wissensmanagement im Unternehmen. in: Schreyögg, G.,Conrad, P. Managementforschung 6: Wissensmanagement. Wiesbaden, Gruyter, S.1-40.
Reich, B. (2006): Die Bilanzierung immateriellen Vermögens nach HGB und IFRS unter besonderer Berücksichtigung von Marken. Oldenburg, Institut für Rechtswissenschaft.

Reichmann, T., Form, S. (2003): Instrumente des Risikomanagement und Risiko-Controlling. in: 18. Deutscher Controlling-Congress, 22. Mai 2003, S.167-188.
Reinhardt, R. (2002): Wissen als Ressource. Theoretische Grundlagen, Methoden und Instrumente zur Erfassung von Wissen. Frankfurt a.M, Lang.
Reitzig, M. (2004): "Strategic Management of Intellectual Property." in: MIT Sloan Management Review 45 (3), S.35-40.
Rencher, A. C. (2002): Methods of multivariate analysis. 2.Auflage, New York, Wiley.
Rentschler, R. (2005): "Kontrolle ist besser." in: IT-Management (1/2), S.22-26.
Riedl, R. (2003): "Begriffliche Grundlagen des Business Process Outsourcing." in: Information Managment & Consulting (18), S.6-10.
Riege, A. (2005): "Three-dozen knowledge-sharing barriers managers must consider." in: Journal of Knowledge Management 9 (3), S.18-35.
Rissbacher, C. (2003): Kooperationen: eine transdisziplinäre Perspektive. Frankfurt a. M., Lang.
Ritchie, B., Brindley, C. (2001): "The information-risk conundrum." in: Marketing Intelligence & Planning 19 (1), S.29-37.
Ritchie, B., Marshall, D. (1993): Business risk management. London, Chapman & Hall.
Rittberger, M. (2004): Vertrauen und Qualität in Informationsdienste. Wo finde ich Vertrauen im Information Quality Framework? in: Hammwöhner, R., Rittberger, M.,Semar, W. Wissen in Aktion. Der Primat der Pragmatik als Motto der Konstanzer Informationswissenschaft. Festschrift für Rainer Kuhlen. Konstanz, UVK Verlagsgesellschaft mbH, S.153-165.
Robertson, M., Hammersley, G. O. (2000): "Knowledge management practices within a knowledge-intensive firm: the significance of the people management dimension." in: Journal of European Industrial Training 24 (2,3,4), S. 241-253.
Rockel, W. (2002): Risikomanagement im Rahmen der Unternehmens- und Konzernüberwachung, Manuskript Nr. 40, Ludwig-Maximilians-Universität München.
Rodgers, W. (2003): "Measurement and reporting of knowledge-based assets." in: Journal of Intellectual Capital 4 (2), S.181-190.
Roehl, H. (2000): Instrumente der Wissensorganisation: Perspektiven für eine differenzierende Interventionspraxis. Wiesbaden, DUV.
Rogulla, M., Walther, H. (2003a): "Effizienz und Sicherheit durch Provisioning." in: kes 6, S.21.
Rogulla, M., Walther, H. (2003b): "Mehr Effizienz und Sicherheit durch Verzeichnisdienste." in: NET- Zeitschrift für Kommunikationsmanagement (11), S.13.
Romeike, F. (2000): " IT-Risiken und Grenzen traditioneller Risikofinanzierungsprodukte." in: Zeitschrift für Versicherungswesen 51 (17), S.603-610.
Romeike, F. (2002): "Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung." in: RATINGaktuell (2), S.12-17.
Romeike, F. (2004a): "Integration des Managements der operationellen Risiken in die Gesamtrisikosteuerung." in: BIT 5 (3), S.41-54.
Romeike, F. (2004b): Lexikon Risiko-Management: 1000 Begriffe rund ums Risiko-Management nachschlagen, verstehen, anwenden. Weinheim, Wiley.
Romhardt, K. (1998): Die Organisation aus der Wissensperspektive: Möglichkeiten und Grenzen der Intervention. Wiesbaden, Gabler.
Rønde, T. (2001): "Trade Secrets and Information Sharing." in: Journal of Economics & Management Strategy 10 (3), S.391-417.
Roos, G., Pike, S., Fernström, L. (2004): Intellectual Capital Management, Measuremement and Disclosure. in: Horváth, P. Intangibles in der Unternehmenssteuerung Strategien und Instrumente zur Wertsteigerung des immateriellen Kapitals. München, Vahlen, S.127-158.
Rosenblatt, Z., Sheaffer, Z. (2001): "Brain drain in declining organizations: toward a research agenda." in: Journal of Organizational Behaviour 22 (4), S.409-424.

Rossa, G. (2004): "User sicher identifizieren, in, 4/2004." in: IT Management (4), S.66-71.
Ruggles, R. L. (1998): "The State of the Notion: Knowledge Management in Practice." in: California Management Review 40 (3), S.80-89.
Rumelt, R. P. (1984): Towards a Strategic Theory of the Firm. in: Lamb, R. B. Competitive Strategic Management. Englewood Cliffs, Prentice Hall, S.556-570.
Rüsberg, L., Süchting, J. (1992): Banken-Rating, Rendite, Risiko und Wachstum von Kreditinstituten, Band 16 der Schriftenreihe des Instituts für Kredit- und Finanzwirtschaft der Ruhr-Universität Bochum Fakultät für Wirtschaftswissenschaften. Wiesbaden, Gabler.
Rusch, G.-K. (2003): "Abschied vom Do-it-Yourself-Prinzip." in: Information Managment & Consulting (18), S.12-16.
Rüstmann, M. (1999): Strategisches Wissensmanagement beim Stellenwechsel. Frensdorf, Digitaldruck.
Rylander, A., Peppard, P. (2005): What Really is a Knowledge-Intensive Firm? - (Re)Framing Research in the “Knowledge Economy”, URL: https://www.som.cranfield.ac.uk/som/research/centres/isrc/documents/WhatisaKIF_Org_Rylander_PeppardwebversionWhatReallyisaKnowledgeIntensiveFirm.pdf, letzter Zugriff: 14.03.2008.
Sabathil, P. (1977): Fluktuation von Arbeitskräften: Determinanten, Kosten und Nutzen aus betriebswirtschaftlicher Sicht. München, Florentz.
Salmela, H. (2003): Assessing the Business Consequences of System Risk. in: ECIS, 2003, Neapel.
Sanchez, R. (1995): Managing articulated knowledge in competence-based competition,
Santomero, A. M. (2003): "Process and Progress in Risk Management." in: Business Review (1), S.1-5.
SAP (2007): Geschäftsbericht 2006, Walldorf.
Sattler, H. (2005): "Markenbewertung: State-of-the-Art." in: Zeitschrift für Betriebswirtschaft (Special Issue 2), S.33-57.
Scandizzo, S. (2005): "Risk mapping and key risk indicators in operational risk management." in: Economic Notes 34 (2), S.231-256.
Schadt, D. (2006): "Über die Ökonomie der IT-Sicherheit Betrachtungen zum Thema "Return on Security Investment"." in: HMD - Praxis der Wirtschaftsinformatik (248), S.16-25.
Schanz, G. (1988): Methodologie für Betriebswirte. 2.Auflage, Stuttgart, Poeschel.
Schermelleh-Engel (2006): Abteilung für Psychologische Methodenlehre: Unterlagen zur Übung Testtheorie und Testkonstruktion Gütekriterien, URL: http://user.uni-frankfurt.de/~moosbrug/, letzter Zugriff: 14.03.2008.
Schierenbeck, H. (1999): Ertragsorientiertes Bankmanagement, Bd. 2, Risiko-Controlling und Bilanzstruktur-Management. 6.Auflage, Gabler.
Schindler, M. (2001): Wissensmanagement in der Projektabwicklung: Grundlagen, Determinanten und Gestaltungskonzepte eines ganzheitlichen Projektwissensmanagements., Lohmar, Eul.
Schindler, M., Eppler, M. J. (2003): "Harvesting project knowledge: a review of project learning methods and success factors." in: International Journal of Project Management 21 (3), S.219-228.
Schmaltz, R., Hagenhoff, S., Kaspar, K. (2004): Information technology support for KM in cooperations. in: The Fifth European Conference on Organizational Knowledge, Learning and Capabilities, Innsbruck.
Schmidt, K. (2006): Der IT-Security-Manager. München, Hanser.
Schmitting, W., Siemes, A. (2003): "Konzeption eines Risikomanagementmodells: Begriffsrahmen und IT-Umsetzung." in: Controller Magazin 6 (3), S.533-540.
Schmitting, W., Siemes, A. (2004): "EDV-technische Unterstützung eines Risikomanagementmodells." in: Controlling (2), S.103-109.

Scholz, C., Bechtel, R. (2002): "Human-Capital-Management Vordenker und mustergültige Unternehmen." in: Personalwirtschaft 29 (1), S.10-11.
Schomann, M., Bloech, J. (2005): Risiken und Risikomanagement im IT-Offshore-Outsourcing. in: Keuper, F. Integriertes Risiko- und Ertragsmanagement. Wiesbaden, Gabler, S.219-245.
Schön, D. (2004): "Risikocontrolling und -management im Projektgeschäft." in: Controlling 16 (4/5), S.287-290.
Schorcht, H. (2004): Risikomanagement und Risikocontrolling junger Unternehmen in Wachstumsbranchen: Konzeption eines theoriegeleiteten Handlungsrahmens für die praxisinduzierte Unternehmenssteuerung. Berlin, Logos.
Schubert, K. (2005): Der Schutz von Know-how, Daten und Informationen nach deutschem Recht, URL: http://www.wissensschutz.de/downloads.html, letzter Zugriff: 14.03.2008.
Schulte, M. (1997): Bank Controlling II: Risikopolitik in Kreditinstituten. Frankfurt a. M., Bankakademie.
Schultz, T. W. (1961): "Investment in Human Capital." in: American Economic Review 51 (1), S.1-17.
Schüppel, J. (1996): Wissensmanagement: organisatorisches Lernen im Spannungsfeld von Wissens- und Lernbarrieren. Wiesbaden, DUV.
Schuy, A. (1989): Risiko-Management: eine theoretische Analyse zum Risiko und Risikowirkungsprozess als Grundlage für ein risikoorientiertes Management unter besonderer Berücksichtigung des Marketing., Frankfurt a. M., Lang.
Schwamborn, S. (1994): Strategische Allianzen im internationalen Marketing: Planung und portfolioanalytische Beurteilung. Wiesbaden, DUV.
Schwartz, D. G. (2006): Aristotelian View of Knowledge Management. in: Schwartz, D. G. Encyclopedia of knowledge management. Hershey, Idea Group, S.11-16.
Seibold, H. (2006): IT-Risikomanagement. München, Oldenbourg.
Sell, A. (1994): Internationale Unternehmenskooperationen. München, Oldenbourg.
Selznick, P. (1957): Leadership in administration, Harper and Row, New York. nachgedruckt in: Foss, N.J. Resources, Firms, and Strategies, Oxford, Oxford Univ. Press.
Senge, P. (1990): "The Leader's New Work: Building Learning Organizations." in: Sloan Management Review 32 (1), S.7-19.
Shapiro, C., Varian, H. R. (1999): Information Rules. A Strategic Guide to the Network Economy. Boston, Harvard Business School Press.
Simister, T. (2000): "Risk management: the need to set standards." in: Balance Sheet 8 (4), S.9-10.
Simon, W. (2002): Systematische Identifikation, Erfassung und Bewertung Operationeller Risiken - eine neue Herausforderung für Banken. in: Eller, R., Gruber, W.,Reif, M. Handbuch Operationelle Risiken: aufsichtsrechtliche Anforderungen, Quantifizierung und Management, Praxisbeispiele. Stuttgart, Schäffer-Poeschel, S.125-152.
Simonin, B. L. (1999): "Ambiguity and the Process of Knowledge Transfer in Strategic Alliances." in: Strategic Management Journal 20 (7), S.595-623.
Simons, R. (1999): "How risky is your company?" in: Harvard Business Review 77 (1), S.85-94.
Sitzberger, S., Nowey, T. (2006): Lernen vom Business Engineering - Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement. in: Lehner, F., Nösekabel, H.,Kleinschmidt, P. Multikonferenz Wirtschaftsinformatik MKWI 2006, Band 2. S.155-165.
Soekijad, M., Andriessen, J. (2004): Mechanisms for knowledge exchange in co-opetitive alliances. in: OKLC 2004, Innsbruck.
Solow, R. M. (1957): Technical change and the aggregate production function.
Song, J., Almeida, P., Wu, G. (2003): "Learning-by-Hiring: When Is Mobility More Likely to Facilitate Interfirm Knowledge Transfer?" in: Management Science 49 (4), S.351-365.

Spender, J. C. (1996): "Making Knowledge the Basis of a Dynamic Theory of the Firm." in: Strategic Management Journal 17 (Winter Special Issue), S.45-62.
Spender, J. C., Grant, R. M. (1996): "Knowledge and the Firm: Overview." in: Strategic Management Journal 17 (Special Issue), S.5-9.
Spira, L. F., Page, M. (2003): "Risk management. The reinvention of internal control and changing role of internal audit." in: Accounting, Auditing & Accountability Journal 16 (4), S.640-661.
Stanek, M. B. (2004): "Measuring alliance value and risk: A model approach to prioritizing alliance projects." in: Management Decision 42 (2), S.182-204.
Starbuck, W. H. (1992): "Learning by Knowledge-Intensive Firms." in: Journal of Management Studies 29 (6), S.713-740.
Staudt, E. (1992): Kooperationshandbuch: ein Leitfaden für die Unternehmenspraxis. Stuttgart, Schaeffer.
Stewart, T. A. (1997): Intellectual Capital. The new wealth of organizations. London, Doubleday.
Stewart, T. A. (1998): Der vierte Produktionsfaktor: Wachstum und Wettbewerbsvorteile durch Wissensmanagement. München, Hanser.
Stickelmann, K. (2002): Operationelles Risiko - Abgrenzung, Definition und Anforderungen gemäß Basel II. in: Eller, R., Gruber, W.,Reif, M. Handbuch Operationelle Risiken: aufsichtsrechtliche Anforderungen, Quantifizierung und Management, Praxisbeispiele. Stuttgart, Schäffer-Poeschel, S.3-41.
Stiemerling, O., Won, M., Wulf, V. (2000): "Zugriffskontrolle in Groupware - Ein nutzerorientierter Ansatz." in: Wirtschaftsinformatik 42 (4), S.318-328.
Stock, W. (2004): "Nutzers Not und Pflichten. Von der Kundenorientierung über das Qualitätsmanagement zum Informations-TÜV." in: Password 05.
Stoi, R. (2003): "Controlling von Intangibles - Identifikation und Steuerung der immateriellen Werttreiber." in: Controlling 15 (3/4), S.38-46.
Strach, P., Everett, A. M. (2006): "Knowledge transfer within Japanese multinationals: building a theory." in: Journal of Knowledge Management 10 (1), S.55-68.
Strassmann, P. A. (1998): "The Value of Knowledge Capital." in: American Programmer 11 (3), S.3-10.
Straub, D. W., Welke, R. J. (1998): "Coping with systems risk: Security planning models for management decision making." in: MIS Quarterly 22 (4), S.441-469.
Strobel, S. (2003): Firewalls und IT-Sicherheit: Grundlagen und Praxis sicherer Netze. Heidelberg, dpunkt.
Strong, D. M., Lee, Y. W., Wang, R. Y. (1997): "10 Potholes in the Road to Information Quality." in: Computer IEEE 30 (8), S.38-46.
Strulik, T. (2001): Die Intelligenz der Risikosteuerung - Wissensmanagement als Management von und durch Komplexität. in: Heimer, T.,Roßbach, P. Management der Ressource Wissen in Banken. Frankfurt a. M., Bankakad., S.31-54.
Suh, B., Han, I. (2003): "The IS risk analysis on a business model." in: Information & Management 41 (2), S.149-158.
Sullivan, P. H. (1999): "Profiting from intellectual capital." in: Journal of Knowledge Management 3 (2), S.132-142.
Sun, P. Y.-T., Scott, J. L. (2005): "An investigation of barriers to knowledge transfer." in: Journal of Knowledge Management 9 (2), S.75-90.
Supekar, K., Patel, C., Lee, Y. (2004): Characterizing Quality of Knowledge on Semantic, in: Web-Proceedings of AAAI Florida AI Research Symposium (FLAIRS-2004), May 17-19, 2004, Miami Beach, Florida, S.1-6.
Sveiby, K.-E., Lloyd, T. (1987): Managing Knowhow. London, Bloomsbury.

Sveiby, K. E. (1996): The Intangible Assets Monitor, URL: http://www.sveiby.com/Portals/0/articles/CompanyMonitor.html, letzter Zugriff: 14.03.2008.
Sveiby, K. E. (1997): The new organizational wealth: managing & measuring knowledge-based assets. San Francisco, Berrett-Koehler.
Sveiby, K. E. (1998): Wissenskapital - das unentdeckte Vermögen: immaterielle Unternehmenswerte aufspüren, messen und steigern. Landsberg/Lech, Verl. Moderne Industrie.
Sveiby, K. E. (2007): "Methods for Measuring Intangible Assets." in.
Sveiby, K. E., Lloyd, T. (1990): Das Management des Know-how: Führung von Beratungs-, Kreativ- und Wissensunternehmen. Frankfurt a. M., Campus.
Swart, J., Kinnie, N. (2003): "Sharing knowledge in knowledge-intensive firms." in: Human Resource Management Journal 13 (2), S.60-75.
Szulanski, G. (1996): "Exploring internal stickiness: impediments to the transfer of best practice within the firm." in: Strategic Management Journal 17 (Winter Special Issue), S.27-43.
Szulanski, G., Jensen, R. J. (2004): "Overcoming stickiness: An Empirical Investigation of the Role of the Template in the Replication of Organizational Routines." in: Managerial and Decision Economic 25 (6-7), S.347-363.
Szulanski, G., Jensen, R. J., Lee, T. (2003): "Adaptation of Know-how for Cross-border Transfer." in: Management International Review 43 (3 Special Issue), S.132-150.
Talaulicar, T. (2004): Wissen. in: Schreyögg, G.,von Weder, A. Handwörterbuch Unternehmensführung und Organisation. 4.Auflage, Stuttgart, Schäffer-Poeschel, S.1640-1647.
Tchankova, L. (2002): "Risk identification - basic stage in risk management." in: Environmental Management and Health 13 (3), S.290-297.
Teece, D. (2000a): "Strategies for managing knowledge assets: the role of firm structure and industrial context." in: Long Range Planning 33 (1), S.35-54.
Teece, D. J. (1976): The multinational corporation and the resource cost of international technology transfer. Cambridge, Ballinger Publishing Company.
Teece, D. J. (2000b): Managing Knowledge Assets in Diverse Industrial Contexts. in: Despres, C.,Chauvel, D. Knowledge horizons: the present and the promise of knowledge management. Boston, S.131-147.
Teece, D. J. (2002): Managing Intellectual Capital. Organizational, Strategic, and Policy Dimensions. Oxford, Oxford Univ. Press.
Teubner, R., Terwey, J. (2005): "IT-Risikomanagement im Spiegel aktueller Normen und Standards." in: HMD: Praxis der Wirtschaftsinformatik 42 (244), S.95–107.
Tewald, C. (2004): "Risikomanagement aus der Isolation im Unternehmen herausführen. Konzeption und Umsetzung erfolgsfaktorenbasierter Balanced Scorecard mit integriertem Risikomanagement." in: Controlling (4/5), S.261-264.
Thiel, C. (2004): "Ein Reifegradmodell für das IT Sicherheitsmanagement." in: HMD - Praxis der Wirtschaftsinformatik (236), S.52-58.
Thomson, S. (2005): Quantifying uncertainty - through modelling operational risk in. in: Reuvid, J. Managing business risk. London, Kogan Page, S.132-140.
Tiebing, O. (2004): "Best Practice Reports Quantifizierung operationeller Risiken." in: BIT 5 (3), S.34-40.
Treleaven, L., Sykes, C. (2005): "Loss of organizational knowledge. From supporting clients to serving head office." in: Journal of Organizational Change Management, 18 (4), S.353-368.
Tsoukas, H., Vladimirou, E. (2001): "What is organizational knowledge?" in: Journal of Management Studies 38 (7), S.973-993.
Ulrich, H. (1984): Management: eine konzentrierte Einführung. Stuttgart, Haupt.
Ulrich, P., Fluri, E. (1995): Management: eine konzentrierte Einführung. Bern, Uni-Taschenbücher.

Unterreitmeier, A., Schwinghammer, F. (2004): Die Operationalisierung von Unternehmenskultur - Validierung eines Messinstruments. Schriften zur Empirischen Forschung und Quantitativen Unternehmensplanung, Nr. 18,

Upadhyaya, S., Raghav Rao, H., Panmanabhan, G. (2006): Secure Knowledge Management. in: Schwartz, D. G. Encyclopedia of knowledge management. Hershey, Idea Group, S.795-801.

van den Brink, G. J. (2001): Operational Risk. Wie Banken das Betriebsrisiko beherrschen. Stuttgart, Schäffer-Poeschel.

Verfassungsschutz (2004a): Landesamt für Verfassungsschutz Baden-Württemberg: Handlungskonzept für Ihren Know-how-Schutz, Stuttgart.

Verfassungsschutz (2004b): Landesamt für Verfassungsschutz Baden-Württemberg: Know-how-Schutz - Handlungsempfehlungen für die gewerbliche Wirtschaft, Stuttgart.

Vile, D. (2007): Secure Mobile Working. Beyond the Technology, Business Community Research Report, URL: http://www.freeformdynamics.com, letzter Zugriff: 14.03.2008.

Völker, J. (2005): BS 7799 Von „Best Practice“ zum Standard, Informationssicherheits-Management nach BS 7799 im Überblick, Secorvo White Paper, URL: http://www.iznnet-kom.niedersachsen.de/IT-Sicherheit/downloads/BS7799_WhitePaper_BS7799_BestPractice_secorvo_27-09-2005.pdf, letzter Zugriff: 14.03.2008.

von Hohnhorst, G. (2002): Anforderungen an das Risikomanagement nach dem KonTraG. in: Hölscher, R.,Elfgen, R. Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken. Wiesbaden, Gabler, S.91-108.

von Krogh, G., Roos, J. (1996): Imitation of Knowledge: a Sociology of Knowledge Perspective. in: von Krogh, G.,Roos, J. Managing Knowledge Perspectives on Cooperation and Competition. London, SAGE, S.32-54.

von Neumann, J., Morgenstern, O. (1953): Theory of games and economic behavior. 3.Auflage, Princeton, Princeton Univ. Press.

von Werder, A. (1992): Risk Management(s), Organisation des. in: Frese, E. Handwörterbuch der Organisation. 3.Auflage, Stuttgart, Schäffer-Poeschel, S.2212-2224.

Voßbein, J. (2006): Zielsetzung und Gebiete von Managementstandards. in: Secure 2006.

Wagner, B. A. (2003): "Learning and knowledge transfer in partnering: an empirical case study." in: Journal of Knowledge Management 7 (2), S.97-113.

Walde, N. (2004): Humankapital-Management: Ansätze zur Bewertung des Wertbeitrags von Mitarbeitern am Beispiel der Lufthansa Technik AG. in: Süssmair, A. Demographie und Wertbeitrag im Fokus des Human Capital Managements. Aachen, Shaker, S.139-289.

Wall, F. (2001): Betriebswirtschaftliches Risikomanagement im Lichte des KonTraG. in: Lange, K. W. Risikomanagement nach dem KonTraG: Aufgaben und Chancen aus betriebswirtschaftlicher und juristischer Sicht. München, Vahlen, S.207-235.

Wallmüller, E. (2004): Risikomanagement für IT- und Software-Projekte. Ein Leitfaden für die Umsetzung in der Praxis. Zürich, Hanser.

Walsh, J. P. u., Ungson, G. R. (1991): "Organizational Memory." in: Academy of Management Review 16 (1), S.57-91.

Wambach, M. (2002): KonTraG und Basel II als Anforderungs-Kriterien für das Risiko-Management im Unternehmen. in: Pastors, P. Risiken des Unternehmens vorbeugen und meistern. München, Hampp, S.213-228.

Wang, R., Strong, D. (1996): "Beyond Accuracy: What Data Quality Means to Data Consumers." in: Journal of Management Information Systems 12 (4), S.5-33.

Wathne, K., Roos, J., Von Krogh, G. (1996): Towards a Theory of Knowledge Transfer in a Cooperative Context. in: Von Krogh, G. Managing knowledge: perspectives on cooperation and competition. London, SAGE, S.55-81.

Wegner, D. M. (1986): A Contemporary Analysis of the Group Mind. in: Mullen, B.,Goethals, C. R. Theories of Group Behavior. New York, Springer, S.185-208.
Wernerfelt, B. (1984): "A Resource-Based View of the Firm." in: Strategic Management Journal 5 (3), S.171-180.
Wernerfelt, B. (1989): "From Critical Resources to Corporate Strategy." in: Journal of General Management International Review 14 (3), S.4-12.
Wetzel, W. (1973): Schließende Statistik. Berlin, de Gruyter.
Wiesmann, A. (2006): "Open-Source-Sicherheitsmanagement. Kosten- und Nutzenfaktoren bei Verwendung von Open Source im Bereich des Information Security Risk Management am Beispiel von SOMAP.org." in: HMD - Praxis der Wirtschaftsinformatik (248), S.62-67.
Wiig, K. M. (1988): Management of Knowledge: Perspectives of a New Opportunity. in: User Interfaces: Gateway or Bottleneck? Proceedings of the Technology Assessment and Management Conference of the Gottlieb Duttweiler Institute Rüschlikon, 20 - 21 Oktober,1986, Amsterdam, S.101-116.
Wiig, K. M. (1997): "Integrating Intellectual Capital and Knowledge Management." in: Long Range Planning 30 (3), S.399-405.
Wildemann, H. (2007): "Strategien gegen Produktpiraterie." in: Industrie Management 23 (2), S.37-40.
Williams, M. (2000): Is a company's intellectual capital performance and intellectual capital disclosure practices related? Evidence from publicly listed companies from the FTSE 100. in: McMasters Intellectual Capital Conference, Toronto.
Williams, R., Bertsch, B., Dale, B., van der Wiele, T., van Iwaarden, J., Smith, M., Visser, R. (2006): "Quality and risk management: what are the key issues?" in: The TQM Magazine 18 (1), S.67-86.
Williams, S. M. (2004): "Downsizing – intellectual capital performance anorexia or enhancement?" in: The Learning Organization 11 (4/5), S.368-379.
Williamson, O. E. (1975): Markets and Hierarchies: Analysis and Antitrust Implications. New York, Macmillan.
Williamson, O. E. (1985): The economic institutions of capitalism: firms, markets, relational contracting. New York, Free Press.
Williamson, O. E. (1990): The firm as a nexus of treaties: an introduction. in: Aoki, M., Gustafsson, B.,Williamson, O. E. The firm as a nexus of treaties. London, Sage, S.1-25.
Willke, H. (1998): Systemisches Wissensmanagement. Stuttgart, Lucius & Lucius.
Wilson, R. L., Rosen, P. A., Al-Ahmadi, M. S. (2006): Secure Knowledge Discovery in Databases. in: Schwartz, D. G. Encyclopedia of knowledge management. Hershey, Idea Group.
Windemann, P., Schlienger, T., Teufel, S. (2006): "Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik." in: HMD - Praxis der Wirtschaftsinformatik (248), S.51-61.
Winter, S., Szulanski, G. (2001): "Replication as Strategy." in: Organization Science 12 (6), S.730-743.
Wirtz, B. W., Göttgens, O., Dunz, M. (2001): "Ansätze zur Markenbewertung." in: Der Markt 40 (4), S.159-167.
Wittmann, W. (1959): Unternehmung und unvollkommene Informationen. Köln, Opladen.
Wolf, E. (2005): IS risks and operational risk management in banks. Lohmar, Eul.
Wolf, K. (2004): "Risikomanagement gemäß den Anforderungen des KonTraG bei Daimler Chrysler." in: Controlling (4/5), S.211-216.
Wolff, E. N. (2005): "The Growth of Information Workers in the U.S. Economy." in: Communications of the ACM 48 (10), S.37-42.

Woolthuis, R. K., Hillebrand, B., Nooteboom, B. (2002): Trust and formal control in interorganizational relationships. ERIM report series research in management, Erasmus Research Institute of Management (ERIM).

Wucknitz, D. U. (2002): Handbuch Personalbewertung: Messgrößen - Anwendungsfelder - Fallstudien. Stuttgart, Schäffer-Poeschel.

Wyss, H.-P. (2000): "Integriertes Risikomanagement. Kontrolle von operativen Risiken - ein wichtiger, oft missachteter Baustein." in: Der Schweizer Treuhänder (3), S.179-184.

Yapp, P. (2003): Information security. in: Jolly, A. Managing business risk. London, S.173-177.

Young, B. (1999): "Raising the standard." in: Operational. Risk - A Risk Special Report (11), S.10-12.

Young, B. R. (2002): New Trends in Information Risk Management. in: Tipton, H. F.,Krause, M. Information Security Management Handbook. Boca Raton, CRC Press.

Zack, M. H. (1999): "Managing Codified Knowledge." in: Sloan Management Review 40 (4), S.45-58.

Zack, M. H. (2003): "Rethinking the Knowledge-Based Organization." in: MIT Sloan Management Review 44 (4), S.67-71.

Zahn, E., Foschiani, S., Tilebein, M. (2000): Nachhaltige Wettbewerbsvorteile durch Wissensmanagement. in: Krallmann, H. Wettbewerbsvorteile durch Wissensmanagement. Methodik und Anwendungen des Knowledge Management. Stuttgart, Schäffer-Poeschel, S.239-270.

Zahra, S. A., George, G. (2002): "Absorptive capacity: a review, reconceptualization, and extension." in: Academy of Management Review 27 (2), S.185-203.

Zander, U., Kogut, B. (1995): "Knowledge and the Speed of the Transfer and Imitation of Organizational Capabilities: An Empirical Test." in: Organization Science 5 (1), S.76-92.

Zbinden, D., Meyer, P. (2001): Wissensrisiko-Management: Ein Vorgehen zur Identifizierung und Bewertung von Wissensrisiken als Problemlösungsinstrument. Discussion Paper 2001-05, Fachhochschule Solothurn, Solothurn.URL: http://www.fhso.ch/pdf/publikationen/dp01-05.pdf, letzter Zugriff: 14.03.2008.

Zech, J. (2002): Integriertes Risikomanagement - Status quo und Entwicklungstendenzen aus der Perspektive eines Versicherungskonzerns. in: Hölscher, R.,Elfgen, R. Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken. Wiesbaden, Gabler, S.33-50.

Zins, C. (2006): "Redefining information science: from "information science" to "knowledge science"." in: Journal of Documentation 62 (4), S.447-461.

zu Kryphausen-Aufseß, D. (2004): Strategisches Management. in: Schreyögg, G. Handwörterbuch Unternehmensführung und Organisation. 4. Auflage.Auflage, Stuttgart, Schäffer-Poeschel, S.1383-1392.

Anhang

A 1 Interviewleitfaden breite Studie

kNOwRISK

Interviewleitfaden zur Studie „Management von Wissensrisiken“

„Wissen wird vielfach als der vierte und bedeutendste Produktionsfaktor bezeichnet. Risiken, die diese Ressource betreffen, finden hingegen bislang nur wenig Beachtung.“

Die Studie „Management von Wissensrisiken“ wird von der Deutschen Forschungsgemeinschaft gefördert und durch den Lehrstuhl für Wirtschaftsinformatik, Betriebliches Informationsmanagement, Universität Halle-Wittenberg unter Projektleitung von Prof. Dr. Ronald Maier durchgeführt.

Ausgangsbasis der Studie bildet eine integrierte Betrachtung des Wandels zur Wissensgesellschaft und der verstärkten Risikoorientierung von Unternehmen. Erstgenannter zeigt sich darin, dass Aktivitäten, Produkte und Dienstleistungen wissensintensiver werden und somit die Bedeutung der Ressource Wissen für Wertschöpfung und Wettbewerbsfähigkeit ansteigt. Daher kommt dem gezielten Management dieser Ressource z.B. in der Form von Mitarbeiterkompetenzen, dokumentierten Erfahrungen oder Patenten eine zentrale Bedeutung zu. Vielfach wurden deshalb Wissensmanagement-Initiativen und entsprechende IT-Systeme eingeführt. Als zweite aktuelle Entwicklung ist eine verstärkte, zum Teil auch regulatorisch bedingte Risikoorientierung (z.B. Basel II, KonTraG, Sarbanes-Oxley) zu beobachten. Diese lässt sich u.a. auf die gestiegene Dynamik des Unternehmensumfeldes, die zunehmende Vernetzung von IT-Systemen sowie einige namhafte Unternehmenskrisen zurückführen. Jedoch erfolgt trotz der hohen Bedeutung von Wissen meist keine explizite und systematische Auseinandersetzung mit Wissensrisiken, sondern primär eine Betrachtung von Kredit- und Marktrisiken. An diesem Defizit setzt diese Studie an.

Ziel der Studie ist die Analyse der Zusammenhänge zwischen der Steuerung von Wissensrisiken und den Konzepten Wissenstransfer, -diffusion, -verlust und -qualität. Die Ergebnisse fließen in Handlungsempfehlungen ein.

Zielgruppe: 120 Unternehmen werden mit Unterstützung der Creditreform entsprechend einer nach Branchen und Größenklassen geschichteten Zufallsstichprobe ausgewählt. Somit sichern Sie mit Ihrer Teilnahme die Repräsentativität der Studie. Zielgruppe für das Telefoninterview ist je Unternehmen ein Mitarbeiter, der einen guten Überblick über die Prozesse des Unternehmens hat. Vorzugsweise ist das Stellenprofil des Ansprechpartners auf die Unternehmenssteuerung, -organisation, -kommunikation oder das Risikomanagement fokussiert. Bitte leiten Sie den Interviewleitfaden gegebenenfalls weiter!

Anonymität: Die Studie dient ausschließlich wissenschaftlichen Zwecken. Sie wird in zwei Stufen durchgeführt. Die Auswertung erfolgt anonymisiert. Die Ergebnisse werden nach Auswertung und Aufbereitung allen Teilnehmern zur Verfügung gestellt.

Erhebung: Das Telefoninterview nimmt ca. 20 Minuten Zeit in Anspruch und ist wie folgt gegliedert:

I) Angaben zum Unternehmen und zur Person
II) Wissensrisiken und deren Steuerung
III) Wissensmanagement und Risikomanagement

Bitte vereinbaren Sie mit uns bis zum 15.12.2006[403] einen Gesprächstermin (+49-345/5523474)! Wir rufen Sie selbstverständlich gerne zum Interview an!

Vielen Dank für Ihre Unterstützung!

[403] Die Deadline wurde im Verlauf der Studie angepasst, solange bis der Rücklauf erreicht war.

I) Angaben zum Unternehmen und zur Person

Branche:

Mitarbeiterzahl: ☐ -9 ☐ 10-49 ☐ 50-249 ☐ 250-999 ☐ ≥ 1000

Ihre Stellenbezeichnung:

Ihre Berufsjahre im Unternehmen:

externe Mitarbeiterfluktuation/Jahr: ☐ ≤ 1% ☐ 2-5% ☐ 6-9% ☐ 10-14% ☐ 15-19% ☐ 20-24% ☐ ≥ 25%

II) Wissensrisiken und deren Steuerung

Bitte beziehen Sie die folgenden Fragen auf das Gesamtunternehmen oder im Falle von Konzernen auf Ihren Unternehmensteil!

		stimme nicht zu	stimme wenig zu	stimme eher wenig zu	mittel	stimme eher zu	stimme zu	stimme stark zu
1.	Der Ressource Wissen kommt in Bezug auf die Erstellung der Wertschöpfung und der Begründung von Wettbewerbsvorteilen eine entscheidende Bedeutung zu.	1	2	3	4	5	6	7
2.	Es ist genau festgelegt, welches Wissen als vertraulich gilt.	1	2	3	4	5	6	7
3.	Der Zugang zu sensitiven Unternehmensbereichen ist physisch stark begrenzt.	1	2	3	4	5	6	7
4.	Der Zugriff auf elektronisch dokumentiertes Wissen wird stark begrenzt.	1	2	3	4	5	6	7
5.	Zugriffsrechte auf elektronisch dokumentiertes Wissen werden in regelmäßigen Zeitabständen oder in Abhängigkeit konkreter Anlässe laufend angepasst.	1	2	3	4	5	6	7
6.	Geheimhaltungsvereinbarungen, die die Weitergabe von Wissen an externe Personen regeln, werden umfassend eingesetzt.	1	2	3	4	5	6	7
7.	Es bestehen klare Richtlinien, welches Wissen über die Unternehmensgrenzen hinaus weitergegeben werden kann (externer Wissenstransfer).	1	2	3	4	5	6	7
8.	Der externe Wissenstransfer ist streng auf ausgewählte Mitarbeiter begrenzt.	1	2	3	4	5	6	7
9.	Konkurrenzschutzklauseln, die eine Abwanderung zu Konkurrenten für einen bestimmten Zeitraum verbieten, werden umfassend als Bestandteil von Arbeitsverträgen eingesetzt.	1	2	3	4	5	6	7
10.	Kooperationsverträge, die den externen Wissenstransfer regeln, werden umfassend als Absicherung eingesetzt.	1	2	3	4	5	6	7
11.	Es bestehen umfassende IT-Sicherheitsrichtlinien für die Mitarbeiter.	1	2	3	4	5	6	7
12.	Die im Rahmen des IT-Sicherheitsmanagements eingeforderten Maßnahmen werden von den Mitarbeitern gewissenhaft umgesetzt.	1	2	3	4	5	6	7
13.	Entwickeltes Wissen wird umfassend durch gewerbliche Schutz- und Urheberrechte (Intellectual Property Rights) geschützt.	1	2	3	4	5	6	7
14.	Abhängigkeiten von Schlüsselkompetenzen einzelner Mitarbeiter werden durch die gezielte Verbreitung dieser Kompetenzen auf mehrere Mitarbeiter stark reduziert.	1	2	3	4	5	6	7

	stimme nicht zu	stimme wenig zu	stimme eher wenig zu	mittel	stimme eher zu	stimme zu	stimme stark zu
15. Durch externen Wissenstransfer wird viel Wissen des Partners erlernt.	1	2	3	4	5	6	7
16. Das durch externen Wissenstransfer erworbene Wissen wird angepasst und trägt zu anderen Projekten, Prozessen bzw. Aufgaben stark bei.	1	2	3	4	5	6	7
17. Im Verlauf der Partnerschaft ist das ursprüngliche Verlassen auf das Wissen bzw. die Abhängigkeit vom Wissen des Partners stark zurückgegangen.	1	2	3	4	5	6	7
18. Die Qualität des durch externen Wissenstransfer erworbenen Wissens ist gut.	1	2	3	4	5	6	7
19. Der Umfang des durch externen Wissenstransfer erworbenen Wissens ist hoch.	1	2	3	4	5	6	7
20. Unautorisierte Zugriffe auf elektronisch dokumentiertes Wissen treten häufig auf.	1	2	3	4	5	6	7
21. Die Abwanderung qualifizierter Mitarbeiter gereicht stark zum Vorteil für Konkurrenten.	1	2	3	4	5	6	7
22. Das den Produkten / Dienstleistungen zugrunde liegende Wissen wird von Konkurrenten schnell rekonstruiert.	1	2	3	4	5	6	7
23. Konkurrenten gelingt es erfolgreich Produkte / Dienstleistungen Ihres Unternehmens zu imitieren.	1	2	3	4	5	6	7
24. Konkurrenten gelingt es in erheblichem Ausmaß vertrauliches Wissen über Ihr Unternehmen zu sammeln.	1	2	3	4	5	6	7
25. Beim externen Wissenstransfer erlangen Partner in erheblichem Ausmaß Zugang zu Wissen, das ihnen aus Gründen der Vertraulichkeit nicht zugänglich sein sollte.	1	2	3	4	5	6	7
26. Im operativen Tagesgeschäft entwickeltes Wissen wird umfassend dokumentiert und verfügbar gemacht.	1	2	3	4	5	6	7
27. In Projekten entwickeltes Wissen wird umfassend dokumentiert und verfügbar gemacht.	1	2	3	4	5	6	7
28. Bei der Nachbesetzung bestehender Stellen treten erhebliche Einarbeitungsprobleme auf, da das erforderliche Wissen nur schwer bzw. unvollständig rekonstruiert werden kann.	1	2	3	4	5	6	7
29. Bei der Vertretung bestehender Stellen treten erhebliche Einarbeitungsprobleme auf, da das erforderliche Wissen nur schwer bzw. unvollständig rekonstruiert werden kann.	1	2	3	4	5	6	7
30. Durch die Reorganisationen von Projektteams, Abteilungen oder Geschäftsbereichen steht Wissen, das benötigt wird, in erheblichem Ausmaß nicht zur Verfügung.	1	2	3	4	5	6	7
31. Dokumentiertes Wissen geht häufig nicht wiederherstellbar verloren.	1	2	3	4	5	6	7

32. Auf dokumentiertes Wissen kann bei Bedarf stetig und ungehindert zugegriffen werden. 1 2 3 4 5 6 7

33. Es ist gut überprüfbar, woher das dokumentierte Wissen stammt bzw. wer verantwortlich ist. 1 2 3 4 5 6 7

34. Dokumentiertes Wissen wird ohne Verzögerung zur Nutzung bereitgestellt. 1 2 3 4 5 6 7

35. Die Korrektheit des dokumentierten Wissens ist hoch. 1 2 3 4 5 6 7

36. Die Aktualität des dokumentierten Wissens ist hoch. 1 2 3 4 5 6 7

37. Von anderen Mitarbeitern dokumentiertes Wissen kann leicht angewandt werden. 1 2 3 4 5 6 7

III) Wissensmanagement und Risikomanagement

38. Besteht für Ihr Unternehmen eine gesetzliche Verpflichtung zum Risikomanagement? ☐ ja ☐ nein

39. Bestehen in Ihrem Unternehmen Risikomanagementinitiativen bzw. setzt man sich gezielt mit Risikomanagement auseinander? ☐ ja ☐ nein

    Seit wann?

40. Bestehen in Ihrem Unternehmen Wissensmanagementinitiativen bzw. setzt man sich gezielt mit Wissensmanagement auseinander? ☐ ja ☐ nein

    Seit wann?

41. Welche weiteren Maßnahmen zur Steuerung von Wissensrisiken setzen Sie ein?

42. Welche drei Maßnahmen zur Steuerung von Wissensrisiken sind Ihrer Ansicht nach am wichtigsten?

Kontakt:
Florian Bayer
Martin-Luther-Universität Halle-Wittenberg
Juristische und Wirtschaftswissenschaftliche Fakultät
Institut für Wirtschaftsinformatik u. OR
Lehrstuhl für Wirtschaftsinformatik, Betriebliches Informationsmanagement
Universitätsring 3
D-06108 Halle / Saale
Tel.: +49-345/5523474 / oder +49-345/5523471 (Sekretariat)
Fax: +49-345/5527374
E-Mail: bayer@wiwi.uni-halle.de
Projektinformationen: http://www.wiwi.uni-halle.de/maier/wissensrisiken

A 2 Interviewleitfaden vertiefende Studie

Allgemeine Fragen[404]	
n = 12	• Welche Maßnahmen können Ihrer Ansicht nach herangezogen werden, um die Risiken der unerwünschten Wissensdiffusion effizient zu steuern? • Welche Kriterien können Ihrer Ansicht nach zur Klassifikation von Wissen herangezogen werden? • In welchen Bereichen sehen Sie Austauschbeziehungen zwischen der Begrenzung von Wissensrisiken einerseits und der Hemmung erwünschter Prozesse andererseits? • Wie könnte die Steuerung von Wissensrisiken in Ihrem Unternehmen implementiert werden?
Clusterspezifische Fragen[405]	
Cluster I **n =2**	• Aus welchen Gründen begrenzen sie vergleichsweise stark den Zugang? • Auf welche Einflussfaktoren ist der vergleichsweise hohe fluktuationsbedingte Wissensverlust zurückzuführen? • Auf welche Einflussfaktoren ist die vergleichsweise hohe wettbewerbsbedingte Diffusion zurückzuführen? • Auf welche Einflussfaktoren ist die vergleichsweise hohe zusammenarbeitsbedingte Diffusion zurückzuführen? • Auf welche Einflussfaktoren ist der vergleichsweise hohe Wissenstransfererfolg zurückzuführen? • Auf welche Einflussfaktoren ist das vergleichsweise hohe Niveau der Wissensqualität zurückzuführen?
Cluster II **n =2**	• Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur IT-Sicherheit? • Auf welche Einflussfaktoren ist der vergleichsweise niedrige Wissenstransfererfolg zurückzuführen? • Auf welche Einflussfaktoren ist das vergleichsweise geringere Niveau der Wissensqualität zurückzuführen?
Cluster III **n =2**	• Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur Begrenzung des Zugangs? • Aus welchen Gründen ergreifen Sie vergleichsweise weniger Maßnahmen zur Kontrolle der Weitergabe? • Aus welchen Gründen ergreifen Sie vergleichsweise mehr Maßnahmen zur IT-Sicherheit und welche Auswirkungen hat dies Ihrer Ansicht nach? • Auf welche Einflussfaktoren ist der vergleichsweise geringe fluktuationsbedingte Wissensverlust zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind?
Cluster IV **n =2**	• Aus welchen Gründen ergreifen Sie vergleichsweise mehr Maßnahmen zur Begrenzung des Zugangs? • Auf welche Einflussfaktoren ist die vergleichsweise geringere zusammenarbeitsbedingte Diffusion zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind? • Auf welche Einflussfaktoren ist die vergleichsweise geringere wettbewerbsbedingte Diffusion zurückzuführen? Werden zusätzliche Steuerungsmaßnahmen ergriffen, die nicht Gegenstand der Studie sind? • Ist die geringere wettbewerbsbedingte Diffusion auf eine vergleichsweise stärkere Kontrolle der Weitergabe zurückzuführen?
Fragen zu positiven Ausprägungen[406]	
n =4	• Auf welche Einflussfaktoren ist das vergleichsweise geringe Risiko des Wissensverlustes in Ihrem Unternehmen zurückzuführen? • Auf welche Einflussfaktoren ist das vergleichsweise geringe Risiko der Wissensdiffusion in Ihrem Unternehmen zurückzuführen? • Auf welche Einflussfaktoren ist der vergleichsweise hohe Wissenstransfererfolg in Ihrem Unternehmen zurückzuführen? • Auf welche Einflussfaktoren ist das vergleichsweise hohe Niveau der Wissensqualität in Ihrem Unternehmen zurückzuführen? • In welchem Zusammenhang zu den ergriffenen Steuerungsmaßnahmen stehen diese Ausprägungen?

[404] Die allgemeinen Fragen wurden allen 12 vertieft untersuchten Unternehmen gestellt.

[405] Die clusterspezifischen Fragestellungen wurden von insgesamt acht Unternehmen beantwortet, wobei je Cluster zwei Unternehmen befragt wurden.

[406] Die Fragen zu den positiven Ausprägungen wurden durch vier Unternehmen mit vergleichsweise positiven Ausprägungen über die vier abhängigen Konzepte hinweg beantwortet.

A 3 Quellen zur Wissensrisikobewertung

Wissensrisiko		Quellen für Risikobewertung
VP1	unbegleiteter Ruhestand	• Personal- bzw. Fluktuationsstatistik
VP2	Beendigung der Erwerbstätigkeit	• Personal- bzw. Fluktuationsstatistik
VP3	Unternehmenswechsel	• Personal- bzw. Fluktuationsstatistik
VP4	fahrlässiges Fehlverhalten	• Dokumentation von Vorfällen • Risikodatenbanken zur Steuerung operationeller Risiken
VP5	vorsätzliches Fehlverhalten	• Dokumentation von Vorfällen • Risikodatenbanken zur Steuerung operationeller Risiken
VO1	Reorganisationsverlust	• Erfassung • Dokumentationen zur Reorganisation
VO2	Nichtdokumentation	• Überprüfung ob Verfahrensanweisungen bestehen bzw. entsprechende Prozesse implementiert sind • (Relation Dokumentation und Projekte)
VO3	Nachfolgeverlust	• Erfassung / Mitarbeiterbefragung
VO4	Vertretungsverlust	• Erfassung / Mitarbeiterbefragung
VO5	Übergabeverlust	• Erfassung / Mitarbeiterbefragung
VO6	Zutrittsverletzung	• Abgleich bestehender Richtlinien mit Standards • Einsatz von Testpersonen
VO7	Zugriffsverletzung	• Abgleich bestehender Richtlinien mit Standards • Penetrationstests
VO8	unbegleitete Beendigung der Zusammenarbeit	• Abbruchquoten von Kooperationen (externe Studien)
VS1	technisches Versagen / Fehlfunktionen	• Auswertung von Logfiles • Dokumentation der IT-Abteilung • Abgleich mit historischen Schadensdatenbanken
VS2	mangelnde Wiederherstellbarkeit	• Dokumentation der IT-Abteilung • Abgleich bestehender Datensicherung mit Standards
VE1	Abwerbung	• Mitarbeiterbefragung • Risikoreporting • Nutzung externer Studien
VE2	Personalausfall	• Personal- bzw. Fluktuationsstatistik
VE3	Diebstahl	• Verlustmeldungen • Nutzung externer Studien (Verluststatistik für Notebooks)
VE4	Angriff auf IT-Systeme	• Auswertung von Logfiles • Dokumentation der IT-Abteilung • externe Statistiken (BSI, CSI/ FBI)
VE5	höhere Gewalt	• Auswertung von Logfiles • Dokumentation der IT-Abteilung • Schadensstatistiken (Rückversicherer)
DP1	fahrlässiges Fehlverhalten	• Dokumentation von Vorfällen • Risikodatenbanken zur Steuerung operationeller Risiken • Kompetenzprofile der Personalabteilung
DP2	vorsätzliches Fehlverhalten	• Dokumentation von Vorfällen • Risikodatenbanken zur Steuerung operationeller Risiken
DO1	Zutrittsverletzung	• Abgleich bestehender Richtlinien mit Standards • Einsatz von Testpersonen • Statistiken über Fälle unautorisierten Zutritts
DO2	Zugriffsverletzung	• Abgleich bestehender Richtlinien mit Standards • Penetrationstests • Statistiken über Fälle unautorisierten Zugriffs
DO3	unkontrollierter Einsatz temporärer beschäftigter Mitarbeiter	• Einsatz von Testpersonen • Statistiken über Fälle des unkontrollierten Einsatzes
DO4	unkontrollierte interorganisatorische Zusammenarbeit	• Einsatz von Testpersonen
DO5	unkontrollierte Veröffentlichung	• Sammlung von Veröffentlichungsquellen und Überprüfung der

		Integration
DS1	Mangelnde Sicherung der IT-Systeme	• Abgleich mit bestehenden Standards
DS2	technisches Versagen / Fehlfunktionen	• Auswertung von Logfiles • Dokumentation der IT-Abteilung • Abgleich mit historischen Schadensdatenbanken
DE1	Aushorchung	• Durchführung von Tests • Statistiken über aufgetretene Fälle • externe Statistiken
DE2	Einschleusung	• Durchführung von Tests • externe Statistiken
DE3	Anwerbung	• Mitarbeiterbefragung • Reporting • externe Statistiken
DE4	opportunistisches Verhalten der Partner	• externe Statistiken • Mitarbeiterbefragung
DE5	unzureichende Vertraulichkeitswahrung durch Partner	• Auswertung vergangener Vorfälle
DE6	Reverse Engineering	• Auswertung vergangener Vorfälle • Nutzung von Schadensstatistiken
DE7	Diebstahl	• Schadensstatistiken • interne Verlustfälle
DE8	Abhören	• entdeckte Abhörgeräte / unterbundene Abhörversuche
DE9	Angriff auf IT-Systeme	• Auswertung von Logfiles • Dokumentation der IT-Abteilung • Abgleich mit historischen Schadensdatenbanken • externe Statistiken / Studien
DE10	Sicherheitsverstoß durch Partner	• Abgleich der Vereinbarungen mit Standards
DE11	Anwendung von Wissen durch ehemalige Mitarbeiter	• aufgetretene Fälle • externe Statistiken
TP1	Zurückhaltung aufgrund Unsicherheit	• Mitarbeiterbefragung
TP2	mangelndes Vertrauen	• Mitarbeiterbefragung
TP3	Abwehr- / Vermeidungshaltung	• Mitarbeiterbefragung
TP4	unzureichende Explizierung	• Kompetenzprofile der Personalabteilung
TP5	unzureichende Absorbierung	• Kompetenzprofile der Personalabteilung
TO1	unbegleitete Reorganisation	• Erfassung • Mitarbeiterbefragung
TO2	unbegleitete Beendigung von Projekten	• Mitarbeiterbefragung
TO3	fehlende Transparenz über vorhandenes Wissen	• Mitarbeiterbefragung
TO4	eingeschränkte Zusammenarbeit	• Mitarbeiterbefragung • Partnerbefragung
TO5	hemmende Sicherheitsrichtlinien	• Mitarbeiterbefragung • Partnerbefragung
TO6	Inkompatibilitäten zwischen den Partnern	• Mitarbeiterbefragung • Partnerbefragung
TS1	Bereitstellung unzureichender Medien	• Mitarbeiterbefragung
TS2	unzureichende Anwenderfreundlichkeit	• Mitarbeiterbefragung
TS3	unzureichende Vertrauenswürdigkeit	• Mitarbeiterbefragung
TE1	mangelnde Leistungsfähigkeit des Partners	• Mitarbeiterbefragung (Kooperationsverantwortliche)
TE2	mangelnde Leistungsbereitschaft des Partners	• Mitarbeiterbefragung (Kooperationsverantwortliche)
TE3	Schutzverhalten des Partners	• Mitarbeiterbefragung (Kooperationsverantwortliche)
QP1	Unzureichende Identifikation und Bewertung	• Kompetenzprofile • Befragung der Führungskräfte
QP2	unzureichende Erstellung und Weiterverarbeitung	• Mitarbeiterbefragung (Kooperationsverantwortliche)
QP3	Manipulation von Inhalten	• Auswertung
QP5	mangelnde Anwendbarkeit von Wissen	• Mitarbeiterbefragung

QO1	unbegleiteter unternehmensinterner Stellenwechsel	• Personal- bzw. Fluktuationsstatistik
QO2	Mangel an qualifiziertem Personal	• Einschätzung Personalabteilung
QO3	mangelnde Verfügbarkeit von Kompetenzen	• Mitarbeiterbefragung • Auswertung vergangener Abhängigkeiten
QO4	unzureichende Gewährleistung der Aktualität	• Mitarbeiterbefragung
QO5	mangelnde inhaltliche Überprüfung	• Mitarbeiterbefragung
QS1	unzureichende Verfügbarkeit von IT-Systemen	• Verfügbarkeitstests • Auswertung von Systemausfällen (Downtime etc.)
QS2	zeitaufwändige Bereitstellung	• Mitarbeiterbefragung
QS3	unzureichend konsolidierte Quellen	• Mitarbeiterbefragung
QS4	unzureichende Vertrauenswürdigkeit	• Mitarbeiterbefragung
QE1	unzureichende Inhaltsqualität der von Dritten bereitgestellten Inhalte	• Mitarbeiterbefragung
QE2	unzureichende Medienqualität der von Dritten bereitgestellten Inhalte	• Mitarbeiterbefragung
QE3	Manipulation der Inhalte durch Dritte	• Mitarbeiterbefragung

A 4 Zusatztabellen zur Auswertung

	anfängliche Eigenwerte		Summen von quadrierten Faktorladungen für Extraktion			rotierte Summe der quadrierten Ladungen			
Komponente	gesamt	% der Varianz	kumulierte %	gesamt	% der Varianz	kumulierte %	gesamt	% der Varianz	kumulierte %
1	8,098	22,493	22,493	8,098	22,493	22,493	4,145	11,515	11,515
2	4,343	12,064	34,557	4,343	12,064	34,557	3,121	8,670	20,185
3	2,413	6,703	41,261	2,413	6,703	41,261	2,755	7,652	27,837
4	2,224	6,179	47,440	2,224	6,179	47,440	2,748	7,632	35,470
5	1,563	4,341	51,780	1,563	4,341	51,780	2,714	7,539	43,009
6	1,463	4,063	55,844	1,463	4,063	55,844	2,448	6,800	49,809
7	1,380	3,834	59,677	1,380	3,834	59,677	2,398	6,661	56,470
8	1,207	3,352	63,030	1,207	3,352	63,030	1,837	5,102	61,572
9	1,069	2,969	65,999	1,069	2,969	65,999	1,594	4,427	65,999
10	,944	2,622	68,621						
11	,925	2,569	71,190						
12	,863	2,398	73,588						
13	,814	2,261	75,849						
14	,740	2,056	77,905						
15	,728	2,024	79,928						
16	,667	1,852	81,780						
17	,625	1,736	83,516						
18	,567	1,576	85,093						
19	,537	1,492	86,585						
20	,487	1,353	87,937						
21	,481	1,336	89,274						
22	,439	1,220	90,494						
23	,405	1,125	91,619						
24	,394	1,093	92,712						
25	,333	,924	93,636						
26	,324	,901	94,537						
27	,271	,753	95,290						
28	,262	,729	96,019						
29	,243	,675	96,694						
30	,213	,591	97,285						
31	,206	,573	97,858						
32	,189	,524	98,381						
33	,166	,462	98,844						
34	,160	,444	99,288						
35	,134	,372	99,660						
36	,122	,340	100,000						

Tab. 94 erklärte Gesamtvarianz (ermittelt in SPSS)

	WIT	KLASS	ZUTB	ZUGB	DYNZ	GHVB	WTRL	BINT	KOS	KOV	ITSR	ITSB	IPR	REDU	EWB	BEIT	REAB	QLEW	QNEW	UZU	NMF	RE	IMI	CI	UZP	NDTG	NDPG	VER	NAB	REO	VDW	VERF	NAVO	REZT	KORR	AKTU	ANWE
WIT	1,00	0,22	0,23	0,28	0,16	0,25	0,12	0,16	0,07	0,05	0,31	0,32	0,19	0,14	0,22	0,36	0,21	0,38	0,47	-0,14	0,09	0,07	0,12	0,05	-0,08	-0,16	-0,20	0,11	0,10	-0,03	-0,15	0,23	0,18	0,24	0,21	0,21	-0,02
KLASS	0,22	1,00	0,41	0,25	0,36	0,42	0,55	0,34	0,25	0,27	0,31	0,32	0,30	0,30	0,19	0,30	0,15	0,20	0,20	0,06	0,17	0,06	0,06	-0,01	0,01	-0,31	-0,30	0,03	-0,12	-0,14	-0,32	0,32	0,33	0,45	0,34	0,37	0,22
ZUTB	0,23	0,41	1,00	0,32	0,40	0,36	0,36	0,33	0,34	0,20	0,41	0,33	0,31	0,13	0,18	0,24	0,16	0,26	0,19	-0,01	0,16	0,11	0,11	0,17	0,06	-0,27	-0,20	0,05	0,06	0,00	-0,23	0,04	0,14	0,14	0,23	0,21	-0,02
ZUGB	0,28	0,25	0,32	1,00	0,46	0,20	0,19	0,51	0,29	0,24	0,19	0,25	0,23	0,04	0,16	0,15	0,30	0,21	0,19	-0,04	0,02	0,17	0,12	0,15	0,10	0,00	-0,18	0,17	0,07	0,09	-0,02	0,02	0,03	0,19	0,15	0,15	-0,03
DYNZ	0,16	0,36	0,40	0,46	1,00	0,25	0,35	0,48	0,38	0,37	0,39	0,38	0,33	0,27	0,31	0,27	0,23	0,21	0,24	0,12	0,22	0,06	0,17	0,12	0,09	-0,19	-0,35	0,11	-0,03	0,04	-0,15	0,15	0,20	0,18	0,33	0,25	0,09
GHVB	0,25	0,42	0,36	0,20	0,25	1,00	0,62	0,38	0,17	0,39	0,39	0,32	0,30	0,32	0,34	0,39	0,11	0,21	0,20	-0,06	0,17	-0,10	-0,09	-0,14	-0,04	-0,28	-0,44	-0,06	-0,08	-0,16	-0,23	0,17	0,20	0,29	0,27	0,34	0,20
WTRL	0,12	0,55	0,36	0,19	0,35	0,62	1,00	0,40	0,32	0,52	0,41	0,44	0,42	0,29	0,27	0,33	0,18	0,13	0,15	0,08	0,16	-0,06	-0,04	-0,01	0,04	-0,38	-0,41	0,00	-0,05	-0,04	-0,16	0,27	0,32	0,33	0,30	0,32	0,26
BINT	0,16	0,34	0,33	0,51	0,48	0,38	0,40	1,00	0,42	0,50	0,22	0,22	0,32	0,19	0,25	0,30	0,23	0,20	0,14	0,04	0,02	-0,11	-0,05	0,01	0,15	-0,23	-0,24	0,06	-0,01	0,04	-0,06	0,20	0,13	0,33	0,23	0,21	0,12
KOS	0,07	0,25	0,34	0,29	0,38	0,17	0,32	0,42	1,00	0,38	0,26	0,22	0,36	0,30	0,18	0,22	0,26	0,15	0,09	0,18	0,16	0,18	0,12	0,22	0,09	-0,25	-0,19	0,16	0,14	0,14	-0,06	0,02	0,04	0,17	0,06	0,12	0,08
KOV	0,05	0,27	0,20	0,24	0,37	0,39	0,52	0,50	0,38	1,00	0,34	0,32	0,50	0,24	0,29	0,36	0,29	0,17	0,05	0,13	-0,03	-0,07	-0,09	-0,06	0,12	-0,28	-0,27	0,16	0,05	0,04	-0,13	0,08	0,06	0,13	0,16	0,15	0,07
ITSR	0,31	0,31	0,41	0,19	0,39	0,39	0,41	0,22	0,26	0,34	1,00	0,62	0,32	0,33	0,24	0,27	0,31	0,25	0,16	0,02	0,04	0,06	0,07	0,02	0,05	-0,30	-0,34	-0,02	-0,07	-0,01	-0,25	0,14	0,18	0,21	0,28	0,23	0,12
ITSB	0,32	0,32	0,33	0,25	0,38	0,32	0,44	0,22	0,22	0,32	0,62	1,00	0,42	0,33	0,26	0,31	0,20	0,26	0,19	-0,02	0,09	0,15	0,11	0,04	0,06	-0,29	-0,26	0,07	-0,07	-0,17	-0,24	0,27	0,21	0,34	0,42	0,26	0,13
IPR	0,19	0,30	0,31	0,23	0,33	0,30	0,42	0,32	0,36	0,50	0,32	0,42	1,00	0,31	0,17	0,15	0,13	0,13	0,09	0,21	0,10	0,11	0,12	0,10	0,14	-0,24	-0,12	0,12	0,01	-0,04	-0,14	-0,04	-0,02	0,05	0,30	0,15	-0,04
REDU	0,14	0,30	0,13	0,04	0,27	0,32	0,29	0,19	0,30	0,24	0,33	0,33	0,31	1,00	0,41	0,36	0,24	0,24	0,23	0,06	0,12	0,11	-0,06	0,03	0,17	-0,25	-0,34	0,00	-0,10	-0,12	-0,17	0,24	0,25	0,39	0,33	0,24	0,19
EWB	0,22	0,19	0,18	0,16	0,31	0,34	0,27	0,25	0,18	0,29	0,24	0,26	0,17	0,41	1,00	0,63	0,22	0,47	0,50	0,07	0,08	-0,06	-0,17	0,03	0,20	-0,11	-0,25	0,22	0,14	-0,05	-0,11	0,14	0,14	0,22	0,30	0,21	0,06
BEIT	0,36	0,30	0,24	0,15	0,27	0,39	0,33	0,30	0,22	0,36	0,27	0,31	0,15	0,36	0,63	1,00	0,21	0,66	0,60	0,10	0,18	0,08	-0,09	0,07	0,11	-0,30	-0,32	0,18	0,17	-0,09	-0,18	0,31	0,26	0,36	0,32	0,31	0,20
REAB	0,21	0,15	0,16	0,30	0,23	0,11	0,18	0,23	0,26	0,29	0,31	0,20	0,13	0,24	0,22	0,21	1,00	0,17	0,14	0,15	-0,10	0,08	0,12	0,11	0,25	-0,11	-0,09	0,08	-0,02	-0,01	-0,15	0,11	0,15	0,22	0,23	0,14	0,23
QLEW	0,38	0,20	0,26	0,21	0,21	0,21	0,13	0,20	0,15	0,17	0,25	0,26	0,13	0,24	0,47	0,66	0,17	1,00	0,67	0,02	0,08	0,08	-0,09	0,08	0,15	-0,26	-0,31	0,14	0,06	-0,05	-0,08	0,19	0,15	0,21	0,26	0,25	0,07
QNEW	0,47	0,20	0,19	0,19	0,24	0,20	0,15	0,14	0,09	0,05	0,16	0,19	0,09	0,23	0,50	0,60	0,14	0,67	1,00	0,12	0,13	0,01	-0,03	0,21	0,19	-0,15	-0,20	0,18	0,07	0,00	-0,11	0,25	0,24	0,27	0,29	0,27	0,05
UZU	-0,14	0,06	-0,01	-0,04	0,12	-0,06	0,08	0,04	0,18	0,13	0,02	-0,02	0,21	0,06	0,07	0,10	0,15	0,02	0,12	1,00	0,19	0,17	0,28	0,50	0,41	0,04	-0,01	0,24	0,15	0,22	0,24	-0,12	-0,04	-0,04	-0,03	-0,16	0,03
NMF	0,09	0,17	0,16	0,02	0,22	0,17	0,16	0,02	0,16	-0,03	0,04	0,09	0,10	0,12	0,08	0,18	-0,10	0,08	0,13	0,19	1,00	0,39	0,43	0,40	0,34	-0,10	-0,17	0,19	0,22	0,17	0,07	0,06	0,08	0,08	-0,02	0,13	0,03
RE	0,07	0,06	0,11	0,17	0,06	-0,10	-0,06	-0,11	0,18	-0,07	0,06	0,15	0,11	0,11	-0,06	0,08	0,08	0,08	0,01	0,17	0,39	1,00	0,63	0,42	0,21	-0,02	-0,05	-0,02	0,12	0,11	0,04	-0,09	-0,06	-0,01	0,00	0,00	0,04
IMI	0,12	0,06	0,11	0,12	0,17	-0,09	-0,04	-0,05	0,12	-0,09	0,07	0,11	0,12	-0,06	-0,17	-0,09	0,12	-0,09	-0,03	0,28	0,43	0,63	1,00	0,56	0,27	0,02	0,00	0,20	0,19	0,26	0,11	-0,08	-0,03	-0,03	0,02	0,03	-0,09
CI	0,05	-0,01	0,17	0,15	0,12	-0,14	-0,01	0,01	0,22	-0,06	0,02	0,04	0,10	0,03	0,03	0,07	0,11	0,08	0,21	0,50	0,40	0,42	0,56	1,00	0,56	-0,04	-0,01	0,30	0,31	0,35	0,19	-0,05	-0,06	-0,02	-0,05	-0,04	-0,14
UZP	-0,08	0,01	0,06	0,10	0,09	-0,04	0,04	0,15	0,09	0,12	0,05	0,06	0,14	0,17	0,20	0,11	0,25	0,15	0,19	0,41	0,34	0,21	0,27	0,56	1,00	0,05	0,06	0,36	0,30	0,35	0,23	-0,14	0,05	-0,01	-0,10	-0,13	-0,03
NDTG	-0,16	-0,31	-0,27	0,00	-0,19	-0,28	-0,38	-0,23	-0,25	-0,28	-0,30	-0,29	-0,24	-0,25	-0,11	-0,30	-0,11	-0,26	-0,15	0,04	-0,10	-0,02	0,02	-0,04	0,05	1,00	0,61	0,13	0,11	0,17	0,28	-0,41	-0,38	-0,45	-0,33	-0,34	-0,27
NDPG	-0,20	-0,30	-0,20	-0,18	-0,35	-0,44	-0,41	-0,24	-0,19	-0,27	-0,34	-0,26	-0,12	-0,34	-0,25	-0,32	-0,09	-0,31	-0,20	-0,01	-0,17	-0,05	0,00	-0,01	0,06	0,61	1,00	0,11	0,08	0,03	0,17	-0,28	-0,35	-0,34	-0,23	-0,26	-0,20
VER	0,11	0,03	0,05	0,17	0,11	-0,06	0,00	0,06	0,16	0,16	-0,02	0,07	0,12	0,00	0,22	0,18	0,08	0,14	0,18	0,24	0,19	-0,02	0,20	0,30	0,36	0,13	0,11	1,00	0,66	0,37	0,25	-0,11	-0,08	-0,03	0,02	-0,07	-0,15
NAB	0,10	-0,12	0,06	0,07	-0,03	-0,08	-0,05	-0,01	0,14	0,05	-0,07	-0,07	0,01	-0,10	0,14	0,17	-0,02	0,06	0,07	0,15	0,22	0,12	0,19	0,31	0,30	0,11	0,08	0,66	1,00	0,53	0,30	-0,15	-0,10	-0,08	-0,09	-0,13	-0,16
REO	-0,03	-0,14	0,00	0,09	0,04	-0,16	-0,04	0,04	0,14	0,04	-0,01	-0,17	-0,04	-0,12	-0,05	-0,09	-0,01	-0,05	0,00	0,22	0,17	0,11	0,26	0,35	0,35	0,17	0,03	0,37	0,53	1,00	0,55	-0,20	-0,20	-0,22	-0,33	-0,34	-0,24
VDW	-0,15	-0,32	-0,23	-0,02	-0,15	-0,23	-0,16	-0,06	-0,06	-0,13	-0,25	-0,24	-0,14	-0,17	-0,11	-0,18	-0,15	-0,08	-0,11	0,24	0,07	0,04	0,11	0,19	0,23	0,28	0,17	0,25	0,30	0,55	1,00	-0,39	-0,34	-0,25	-0,34	-0,45	-0,23
VERF	0,23	0,32	0,04	0,02	0,15	0,17	0,27	0,20	0,02	0,08	0,14	0,27	-0,04	0,24	0,14	0,31	0,11	0,19	0,25	-0,12	0,06	-0,09	-0,08	-0,05	-0,14	-0,41	-0,28	-0,11	-0,15	-0,20	-0,39	1,00	0,60	0,68	0,43	0,50	0,39
NAVO	0,18	0,33	0,14	0,03	0,20	0,20	0,32	0,13	0,04	0,06	0,18	0,21	-0,02	0,25	0,14	0,26	0,15	0,15	0,24	-0,04	0,08	-0,06	-0,03	-0,06	0,05	-0,38	-0,35	-0,08	-0,10	-0,20	-0,34	0,60	1,00	0,58	0,37	0,48	0,38
REZT	0,24	0,45	0,14	0,19	0,18	0,29	0,33	0,33	0,17	0,13	0,21	0,34	0,05	0,39	0,22	0,36	0,22	0,21	0,27	-0,04	0,08	-0,01	-0,03	-0,02	-0,01	-0,45	-0,34	-0,03	-0,08	-0,22	-0,25	0,68	0,58	1,00	0,52	0,46	0,39
KORR	0,21	0,34	0,23	0,15	0,33	0,27	0,30	0,23	0,06	0,16	0,28	0,42	0,30	0,33	0,30	0,32	0,23	0,26	0,29	-0,03	-0,02	0,00	0,02	-0,05	-0,10	-0,33	-0,23	0,02	-0,09	-0,33	-0,34	0,43	0,37	0,52	1,00	0,65	0,40
AKTU	0,21	0,37	0,21	0,15	0,25	0,34	0,32	0,21	0,12	0,15	0,23	0,26	0,15	0,24	0,21	0,31	0,14	0,25	0,27	-0,16	0,13	0,00	0,03	-0,04	-0,13	-0,34	-0,26	-0,07	-0,13	-0,34	-0,45	0,50	0,48	0,46	0,65	1,00	0,33
ANWE	-0,02	0,22	-0,02	-0,03	0,09	0,20	0,26	0,12	0,08	0,07	0,12	0,13	-0,04	0,19	0,06	0,20	0,23	0,07	0,05	0,03	0,03	0,04	-0,09	-0,14	-0,03	-0,27	-0,20	-0,15	-0,16	-0,24	-0,23	0,39	0,38	0,39	0,40	0,33	1,00

Tab. 95 Korrelationsmatrix (ermittelt in SPSS)